ALTUSCN™
Enterprise Solutions by ATEN

CCVSR Video Session Recorder

User Manual

www.aten.com

FCC Information

This is an FCC Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

RoHS

This product is RoHS compliant.

SJ/T 11364-2006

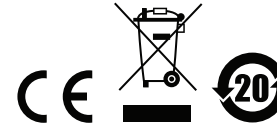
The following contains information that relates to China.

部件名称	有毒有害物质或元素					
	铅	汞	镉	六价铬	多溴联苯	多溴二苯醚
电器部件	●	○	○	○	○	○
机构部件	○	○	○	○	○	○

○: 表示该有毒有害物质在该部件所有均质材料中的含量均在SJ/T 11363-2006规定的限量要求之下。

●: 表示符合欧盟的豁免条款，但该有毒有害物质至少在该部件的某一均质材料中的含量超出SJ/T 11363-2006的限量要求。

×: 表示该有毒有害物质至少在该部件的某一均质材料中的含量超出SJ/T 11363-2006的限量要求。



User Information

Online Registration

Be sure to register your product at our online support center:

International	http://support.aten.com
North America	http://www.aten-usa.com/product_registration

Telephone Support

For telephone support, call this number:

International	886-2-8692-6959
China	86-10-5255-0110
Japan	81-3-5615-5811
Korea	82-2-467-6789
North America	1-888-999-ATEN ext 4988
United Kingdom	44-8-4481-58923

User Notice

All information, documentation, and specifications contained in this manual are subject to change without prior notification by the manufacturer. The manufacturer makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties as to merchantability or fitness for any particular purpose. Any of the manufacturer's software described in this manual is sold or licensed *as is*. Should the programs prove defective following their purchase, the buyer (and not the manufacturer, its distributor, or its dealer), assumes the entire cost of all necessary servicing, repair and any incidental or consequential damages resulting from any defect in the software.

The manufacturer of this system is not responsible for any radio and/or TV interference caused by unauthorized modifications to this device. It is the responsibility of the user to correct such interference.

The manufacturer is not responsible for any damage incurred in the operation of this system if the correct operational voltage setting was not selected prior to operation. PLEASE VERIFY THAT THE VOLTAGE SETTING IS CORRECT BEFORE USE.

Package Contents

Basic Package

The Video Session Recorder package consists of:

1 Video Session Recorder USB License Key

1 Software CD

1 User Instructions*

Check to make sure that all of the components are present and in good order. If anything is missing, or was damaged in shipping, contact your dealer.

Read this manual thoroughly and follow the installation and operation procedures carefully to prevent any damage to the switch or to any other devices on the Video Log Server installation.

***** Features may have been added to the Video Log Server since this manual was published. Please visit our website to download the most up-to-date version.

Copyright © 2013 ATEN® International Co., Ltd.
F/W Version: V1.0.062
Manual Date: 2013-05-28

Altusen and the Altusen logo are registered trademarks of ATEN International Co., Ltd. All rights reserved. All other brand names and trademarks are the registered property of their respective owners.

Contents

FCC Information ii
SJ/T 11364-2006. ii
User Information iii
Online Registration iii
Telephone Support iii
User Notice iii
Package Contents. iv
Basic Package. iv
About This Manual ix
Conventions x
Product Information. x

Chapter 1.
Introduction
Overview 1
Features 2
Requirements 3
Computer. 3
KVM Over the NET™ Switch 3
Browsers 3
Licenses 4
Primary Servers. 4
Secondary Servers 4
Archive Servers 4
Nodes 4
License Options. 5
Add Node Options 6

Chapter 2.
VSR Installation
Overview 7
Installing the VSR Software 7
Starting the Installation 7
Licenses 9

Chapter 3.
VSR Application
Overview 10
VSR Login 10
The VSR Main Page 13
Sessions 13
System Log 14
Settings 15
Server Type 15

Service Ports 16
Archive Server 16
Disable Keystroke Recording 16
Maintenance 17
Backup 17
Restore 17
License 18
Upgrading the License 18

Chapter 4.
VSR Archive Server
Overview 19
Installing the VSR Archive Server 19
Starting the Installation 19
Licenses 22
Archive Server GUI 23
Setup 23
Playback 24
Begin Time/End Time 24
Search Filter 24
Play Selected 25
Export/Import 26
Begin Time/End Time 26
Device Name 26
Search File 27
Export File 27
Export & Delete 27
Delete File 27
Import File 27
Storage 28
Settings 29
License 30

Chapter 5.
The User Interface
Overview 31
Browser Login 31
The Web Browser Main Page 32
Page Components 32
The Tab Bar 33

Chapter 6.
Playback
Overview 35
Search Video 35
Port List 36

Playback 36
Advanced Search 37
Playback 37
Sessions 38
Video Log Viewer 39
Toolbar 39

Chapter 7.

User Management

Users 43
Adding Users 43
Modifying User Accounts 46
Deleting User Accounts 46
Groups 47
Creating Groups 47
Modifying Groups 48
Deleting Groups 49
Users and Groups 50
Assigning Users to a Group From the User's Notebook 50
Removing Users From a Group From the User's Notebook 51
Assigning Users to a Group From the Group's Notebook 52
Removing Users From a Group From the Group's Notebook 53
Device Assignment 54
Assigning Device Permissions From the User's Notebook 54
Assigning Device Permissions From the Group's Notebook 55
System Permissions 56
Assigning System Permissions From the User's Notebook 56
Assigning System Permissions From the Group's Notebook 57

Chapter 8.

Device Management

Overview 58
Recording KVM Ports 58
Adding KVM Devices 59
Configuring KVM Ports 60
Deleting KVM Devices 61

Chapter 9.

Logs

Overview 62
Latest Logs 62
Search Logs 63
Notification Settings 65

Chapter 10.
System Management

Overview . . . 66
System Info . . . 67
VSR-Local . . . 67
Network . . . 68
ANMS . . . 69
Event Destination . . . 69
Authentication . . . 71
Security . . . 74
Login Failures . . . 74
Filter . . . 75
Account Policy . . . 77
Private Certificate . . . 78
Certificate Signing Request . . . 79
Video Session Recorder . . . 81
Adding Secondary VSR Servers . . . 81
Deleting Secondary VSR Servers . . . 82
Enable/Disable Secondary VSR Servers . . . 82
Maximum Recording Time . . . 82
Log Servers . . . 83

Chapter 11.
Preferences

Overview . . . 84

Appendix

Safety Instructions . . . 86
General . . . 86
Technical Support . . . 88
International . . . 88
North America . . . 88
USB Authentication Key Specifications . . . 89
Supported KVM Over the NET™ Switches . . . 89
Windows XP Installation . . . 90
Trusted Certificates . . . 91
Overview . . . 91
Self-Signed Private Certificates . . . 92
Examples . . . 92
Importing the Files . . . 92
Limited Warranty . . . 93

About This Manual

This User Manual is provided to help you get the most from your Video Log Server system. It covers all aspects of installation, configuration and operation. An overview of the information found in the manual is provided below.

Chapter 1, *Introduction*, introduces you to the Video Session Recorder application. Its purpose, features, benefits, and requirements are presented.

Chapter 2, *VSR Installation*, provides step-by-step instructions for installing the Video Session Recorder software.

Chapter 3, *VSR Application*, describes how to use the VLog application, and explains it's features and function.

Chapter 4, *VSR Archive Server*, describes how to use the VSR Archive Server, and explains it's features and function.

Chapter 5, *The User Interface*, explains how to login to the Video Session Recorder using a web browser.

Chapter 6, *Playback*, explains how to use the features and functions of the Playback page, used to search and play video log files.

Chapter 7, *User Management*, shows super administrators and administrators how to create, modify, and delete users and groups, and assign attributes to them.

Chapter 8, *Device Management*, shows super administrators how to add KVM devices and configure ports on the Video Session Recorder, in order to record video logs.

Chapter 9, *Logs*, shows how to use the log file utilities to view the events that take place on the Video Session Recorder.

Chapter 10, *System Management*, explains how to use the System Management page to configure *System Information, Network, ANMS, Security*, and the *Video Session Recorder* settings.

Chapter 11, *Preferences*, explains how to set custom preferences for the user currently logged in.

An Appendix, at the end of the manual provides technical and troubleshooting information.

Conventions

This manual uses the following conventions:

Monospaced	Indicates text that you should key in.
[ ]	Indicates keys you should press. For example, [Enter] means to press the **Enter** key. If keys need to be chorded, they appear together in the same bracket with a plus sign between them: [Ctrl+Alt].
1.	Numbered lists represent procedures with sequential steps.
♦	Bullet lists provide information, but do not involve sequential steps.
→	Indicates selecting the option (on a menu or dialog box, for example), that comes next. For example, Start → Run means to open the *Start* menu, and then select *Run*.
	Indicates critical information.

Product Information

For information about all ALTUSEN products and how they can help you connect without limits, visit ALTUSEN on the Web or contact an ALTUSEN Authorized Reseller. Visit ALTUSEN on the Web for a list of locations and telephone numbers:

International	http://www.aten.com
North America	http://www.aten-usa.com

Chapter 1
Introduction

Overview

The Video Session Recorder is ATEN's innovative software which was developed to work with ALTUSEN KVM Over the NET™ products to securely and reliably record the video and operation of computers which are connected through KVM ports. Not only does the software record a video of the screen display but also logs operations such as key-strokes and mouse clicks. The software can be managed to record specific server ports automatically for convenient auditing and safe management.

The Video Session Recorder supports the recording of multiple KVM Over the NET™ switches, and up to 12 active KVM ports can be recorded at the same time. With the specialized video player tool, encrypted file formats, and user permission settings; only authorized users can view, search, and delete recorded videos and operational logs, ensuring the highest level of security with customized management for automated functionality.

Furthermore, the Video Session Recorder offers powerful search capabilities; the recorded videos and operation logs can be searched by time, device, or port. When playing searched recordings, in addition to the video image, the screen also shows the operations (mouse clicks and key-strokes) being made by the user logged into the computer, arranged in order of recorded time, for easy monitoring, and boosting the efficiency of detailed management and auditing.

The Video Session Recorder is a great tool to create reference and instructional type videos. For instance, if a complex update is required across field office servers, administrators can quickly generate a step by step instructional video with the exact key-strokes and mouse clicks shown on the screen. The administrator can then send the video to branch offices for implementation, instantly reducing training and support time. Videos can be created for software and network training or implementation; installations, configurations and system updates or any computer related instructions. Another advantage is that videos are created and saved automatically when the KVM port is accessed, and are password protected for security.

By integrating the Video Session Recorder into your KVM installation, you can automate the security of your server room and make auditing an effective tool.

Features

- Automatically create complete recordings of a computer's operations when remote users access a KVM port – which are saved to an indexed database for advanced searches
- Supports high quality video recordings – with a video resolution up to 1600 x 1200 with 16 bit color depth
- Supports recording on multiple KVM Over the NET™ Switches
- Simultaneously records and plays the operation of multiple KVM ports*
- Search functions with keyword filters for video recordings
- Special video player tools with format, video record exporting, and password protection for enhanced security
- IP Filter for enhanced protection
- System event notification via SMTP email; SNMP trap and Syslog support
- Configurable user and group permissions – for search, play, system management, record management, and save management
- Port level permissions – users can only view ports they have been authorized on
- Supports device level event logs
- Archive Server Support
- Multilanguage GUI Supports: English, Traditional Chinese, Simplified Chinese, Japanese, and Korean
- Automatically runs software as daemon service in the background
- Multi-browser support: Internet Explorer, Chrome, Firefox, Safari, Opera, Mozilla, Netscape
- Supports SSL 128-bit data encryption and RSA 1024-bit certificates for secure web browser logins
- 3rd party remote authentication supports: RADIUS, LDAP, LDAPS, and MS AD Directory

*Up to 12 KVM sessions can be recorded at one time when the recommend hardware requirements of the CCVSR server are met.

Requirements

Computer

Systems that the Video Session Recorder will be installed on should meet the following requirements:

- Hardware Requirements
  - Minimum/4 video sessions: Intel® Pentium 4, 2.6GHz, 2G RAM
  - Maximum/12 video sessions: Intel® Intel Core™ i5, 2.5GHz, 4G RAM
  - Hard drive: 500MB or more free space
  - Ethernet: At least 1 Ethernet adapter (100Mbps or higher) – Giga LAN recommended
- Operating System Requirements:
  - Windows: XP, 7, 2003, 2008

KVM Over the NET™ Switch

Computers recorded by the Video Session Recorder must be connected to a port on a KVM Over the NET™ Switch (see *Supported KVM Over the NET™ Switches*, page 89).

Browsers

Supported browsers for users that log into the Video Session Recorder include the following:

Browser	Version
Chrome	20.0.1 and higher
IE	6 and higher
Firefox	1.5 and higher
Mozilla	1.7 and higher
Netscape	8.1 and higher
Opera	11.64 and higher
Safari	6.0 and higher

Licenses

The CCVSR license controls the number of Primary Servers, Secondary Servers, Archive Servers and nodes permitted on the CCVSR installation. License information is contained on the USB License Key that came with your CCVSR purchase. For a sample deployment see *CCVSR Deployment Example:*, page 5, for details.

Upon completion of the CCVSR software installation, the number of licenses that you purchased is automatically added. To add anything more, you must upgrade the license. See *Upgrading the License*, page 172, for detailed information.

Primary Servers

Management - A Primary Server is the central management software used to record, view, and manage all aspects of a CCVSR installation. All Secondary Servers, Archive Servers, and Nodes work through the Primary Server.

Secondary Servers

Storage - Secondary Servers reduce the work load and provide extended storage for the Primary Server - with limited configuration functionality.

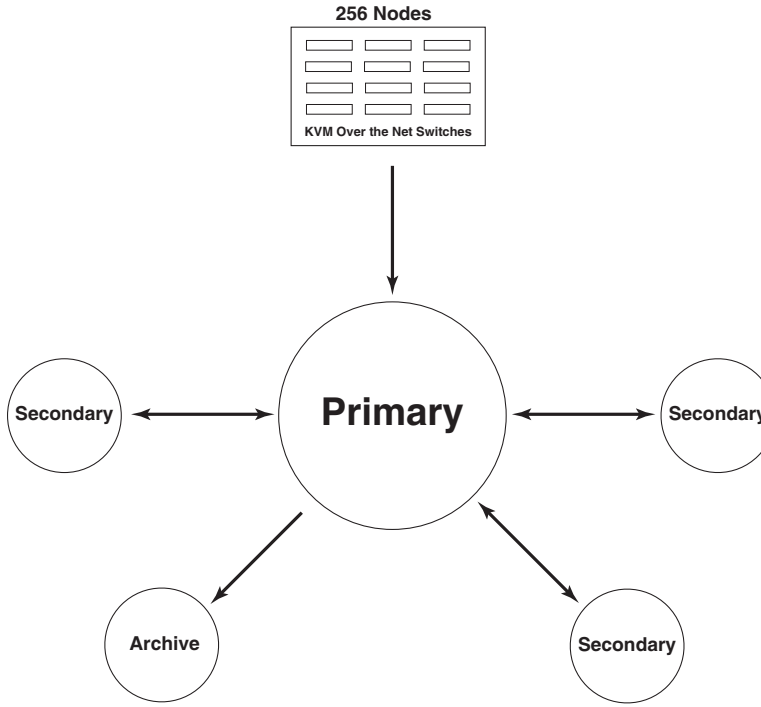
Archive Servers

Archive - The Archive Server automatically archives all video log files created on the Primary Server into a separate organized database for extended backup and viewing. The Archive Server allow you to import, export, and allocate large databases separate from the VSR system.

Nodes

KVM Ports - A node is a physical port on a KVM Over the NET™ Switch. Each node you want to record video logs on requires a license.

CCVSR Deployment Example:



License Options

Model	Node	Primary
CCVSR8	8	1
CCVSR16	16	1
CCVSR32	32	1
CCVSR64	64	1
CCVSR128	128	1
CCVSR256	256	1
CCVSR512	512	1
CCVSR1024	1024	1
CCVSR2048	2048	1
CCVSRUnlimited	Unlimited	1

Add Node Options

Add License Model	Nodes
CCVSRN1	1
CCVSRN8	8
CCVSRN16	16
CCVSRN32	32
CCVSRN64	64
CCVSRN128	128
CCVSRN256	256
CCVSRN512	512
CCVSRN1024	1024
CCVSRN2048	2048

Chapter 2
VSR Installation

Overview

This chapter describes how to install the Video Session Recorder (VSR) software on a computer. The VSR application runs background services for the Video Session Recorder to operate and is used to set basic server configurations. The VSR application must be running for the Video Session Recorder's web browser features to work.

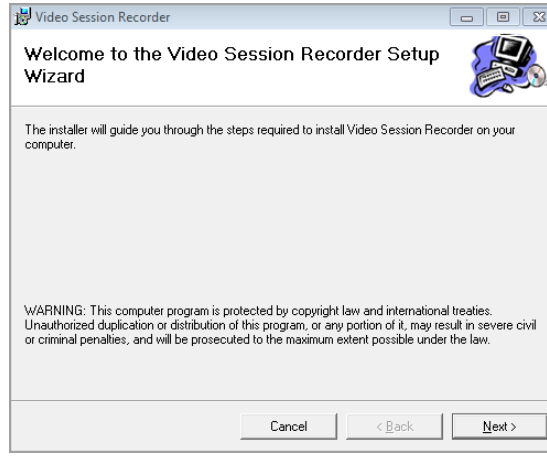
Installing the VSR Software

Starting the Installation

To install the VSR application on a Windows system, do the following:

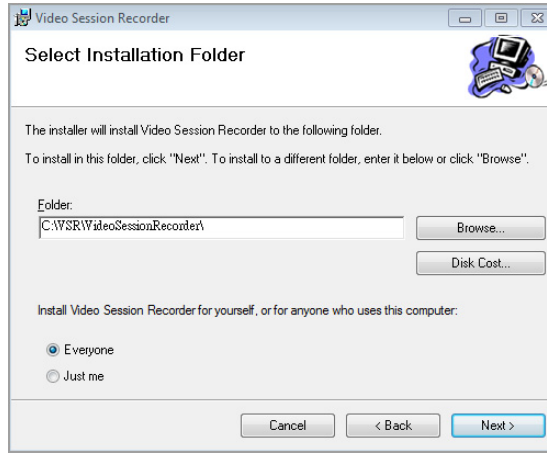
> If you are installing on a computer running Windows XP, you must first install IPv6. See *Windows XP Installation*, page 90, for details.

1. Put the software CD that came with your package into the computer's CD drive.
2. Go to the folder where the *setup.exe* file is located, and execute it. A screen, similar to the one below, appears:


Video Session Recorder
Welcome to the Video Session Recorder Setup Wizard
The installer will guide you through the steps required to install Video Session Recorder on your computer.
WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.
Cancel
< Back
Next >

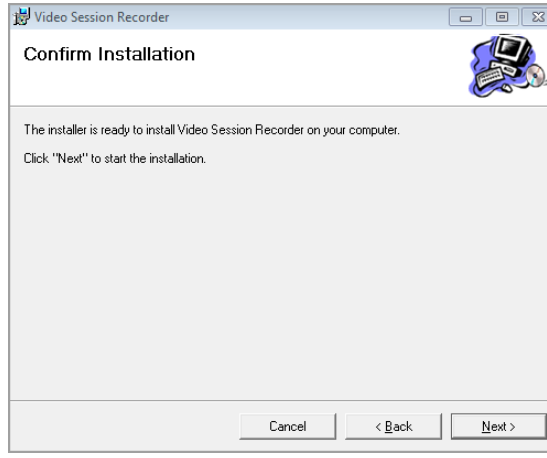
Click **Next** to continue.

3. On the *Select Installation Folder* page, specify the installation folder, or click **Browse** to choose the location where you want to install it. Then choose if you want to install it for yourself (**Just me**), or for anyone who uses this computer (**Everyone**). Click **Disk Cost** to view available drives and disk space.

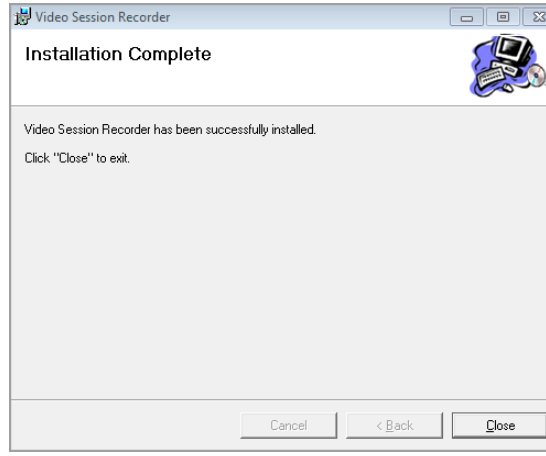

Video Session Recorder
Select Installation Folder
The installer will install Video Session Recorder to the following folder.
To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".
Folder:
C:\WSR\VideoSessionRecorder\
Browse...
Disk Cost...
Install Video Session Recorder for yourself, or for anyone who uses this computer:
Everyone
Just me
Cancel
< Back
Next >

Click **Next** to continue.

4. The *Confirm Installation* window appears, click **Next** to continue:


Video Session Recorder
Confirm Installation
The installer is ready to install Video Session Recorder on your computer.
Click "Next" to start the installation.
Cancel
< Back
Next >

5. When the installation is complete the following message will appear:



Licenses

Upon completion of the VSR software installation, a default license for one server is automatically provided. To add more Video Session Recorders, you must upgrade the license. To upgrade the license, See *License*, page 18, for details. For License options See *License Options*, page 5, for details.

Chapter 3
VSR Application

Overview

The Video Session Recorder (VSR) application runs background services for the Video Session Recorder's browser interface to operate and allows you to view logs, set basic server configurations, and run backup/restore maintenance tasks. The VSR application starts the services that run the Video Session Recorder, and allow the management functions within a web browser session (see Chapter 5, *The User Interface*). This chapter describes the VSR application's features.

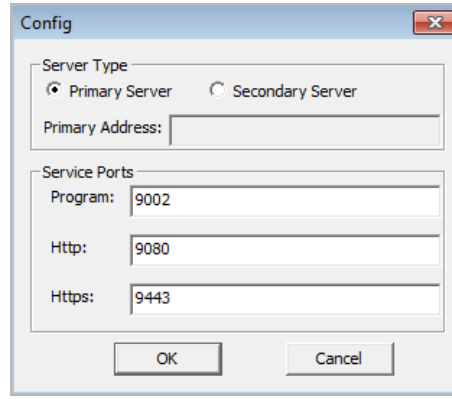
VSR Login

To start VSR and login to the application, do the follow:

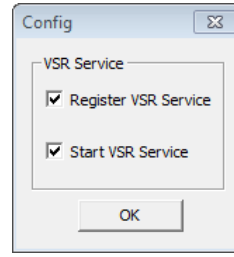
1. Double click the VSR shortcut from the Start Menu or desktop:

   A VSR icon like the one above will appear in the taskbar, after step 2 is complete.

2. The first time you open the VSR application the *Config Server Type* screen appears (see *Server Type*, page 15, for details), set the type and click **OK**.



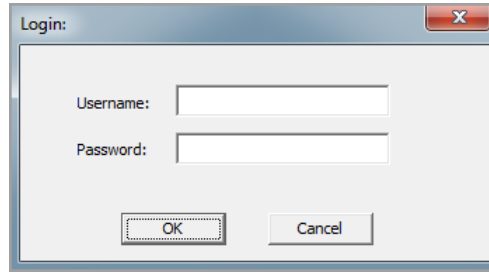
3. The **Config** dialog box appears with two *VSR Service* options, as shown:



Register VSR Service: This option installs and registers the VSR Service with the Windows operating system so that it can run the software in the background.

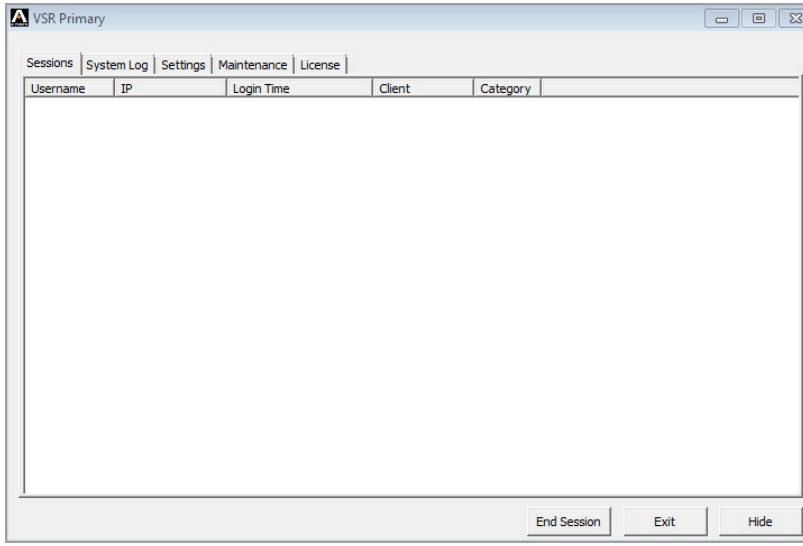
Start VSR Service: This option will start the VSR Service automatically after the installation is complete.

4. Next, click the VSR icon from the taskbar. When the authentication screen appears on the monitor, enter the username and password:



Since this is the first time you are logging in, use the default Username: *administrator*; and the default Password: *password*. Click **OK**.

5. Once you are logged in, the main page appears:

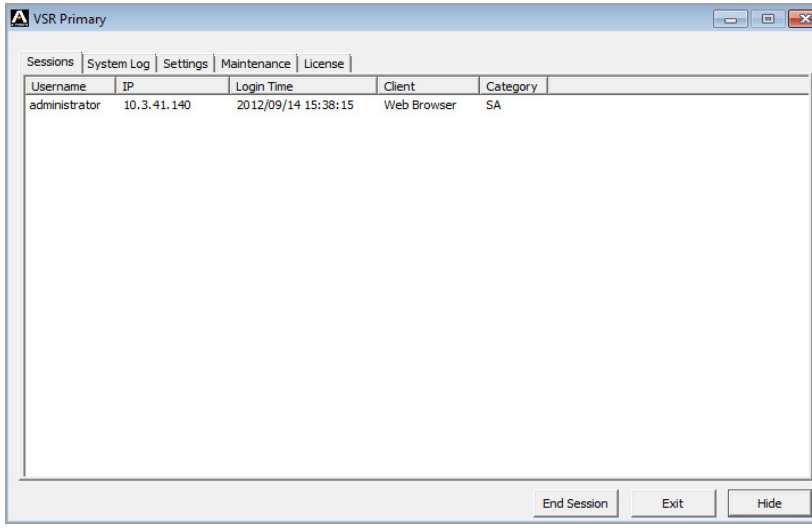


The VSR Main Page

When the VSR application opens you have 5 tabs to choose from: *Sessions*, *System Log*, *Settings*, *Maintenance*, and *License*. From each tab you can *Exit* to logout and shut down the VSR application- stopping all Video Session Recorder services, or *Hide* to logout and continue running the VSR application while minimized to the task bar. Anytime you need to *Save* your settings, VSR will automatically shutdown to allow the changes to take affect, and you will need to restart the application.

Sessions

The Session tab lets you see at a glance which users are currently logged into the main Video Session Recorder's browser interface, and provides information about each session.

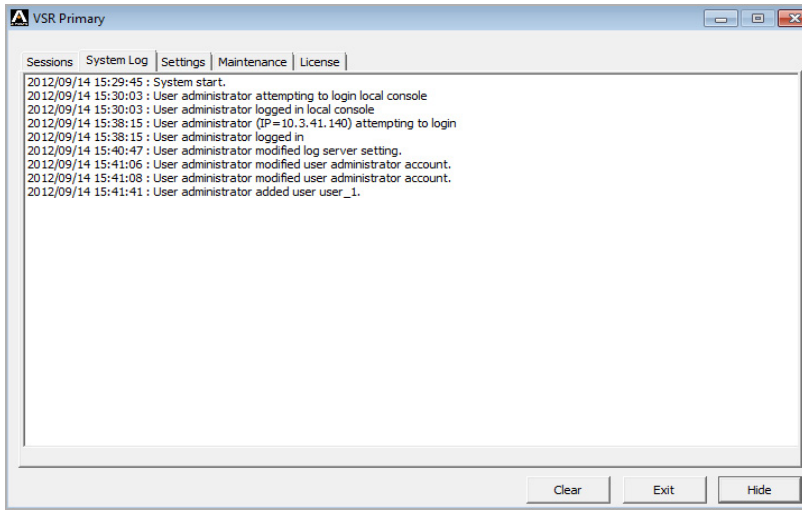


The meanings of the column headings are fairly straightforward. The *IP* heading refers to the IP address that the user has logged in from, the *Login Time* shows when the user logged in to the Video Session Recorder, and the *Category* displays the type of user that logged in.

This page also gives the administrator the option of forcing a user logout by selecting the user and clicking **End Session** at the bottom of the page.

System Log

The System Log tab provides a detailed log of events taking place on the Video Session Recorder.

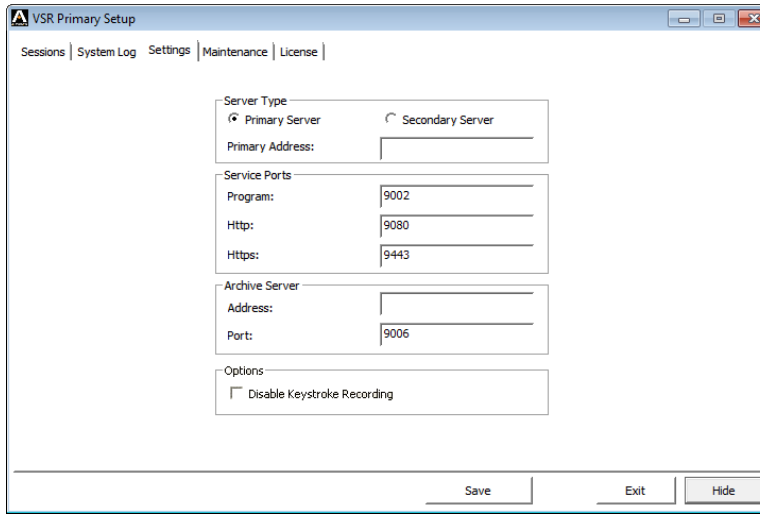

VSR Primary
Sessions
System Log
Settings
Maintenance
License
2012/09/14 15:29:45 : System start.
2012/09/14 15:30:03 : User administrator attempting to login local console
2012/09/14 15:30:03 : User administrator logged in local console
2012/09/14 15:38:15 : User administrator (IP=10.3.41.140) attempting to login
2012/09/14 15:38:15 : User administrator logged in
2012/09/14 15:40:47 : User administrator modified log server setting.
2012/09/14 15:41:06 : User administrator modified user administrator account.
2012/09/14 15:41:08 : User administrator modified user administrator account.
2012/09/14 15:41:41 : User administrator added user user_1.
Clear
Exit
Hide

The System Log provides a breakdown of time, user, and a description of each event occurring. The log file tracks a maximum of 512 events. When the limit is reached, the oldest events get discarded as new events come in.

You can clean all System logs by clicking **Clear.**

Settings

The settings tab is used to determine how the Video Session Recorder functions on the local machine: as a *Primary Server* or *Secondary Server*, and has two sections.



Server Type

Primary Server
Select *Primary Server* for a computer that is running as the main Video Session Recorder. This computer will host and manage all aspects of the Video Session Recorder, and can add computers running as *Secondary Servers* for extended storage of video log files.

Secondary Server
Select *Secondary Server* if the computer is being used as storage space for video log files from a *Primary Server*. As a *Secondary Server*, it's only function will be to store video log files for the *Primary Server,* and when you login to the VSR application only the *Settings* tab is available. If you choose this option, provide the following information:

Primary Address- input the IP address of a computer running as the *Primary* Video Session Recorder.

Service Port: input the Program Service Port number of the *Primary Server.* The default service port for this feature is 9002.

The Secondary Server must be added to the *Primary Server* in order to work. *See Video Session Recorder*, page 81, for details.

Service Ports

As a security measure, if a firewall is being used, the Administrator can specify the port numbers that the firewall will allow. If a port other than the default is used, users must specify the port number as part of the IP address when they log in. If an invalid port number (or no port number) is specified, the Video Session Recorder will not be found. An explanation of the fields is given in the table below:

Field	Explanation
Program	This is the port number to configure on a *Secondary Server* to connect to a *Primary Server* hosting the Video Session Recorder (see page 15 for details). The default is 9002.
HTTP	The port number for a browser login. The default is 9080.
HTTPS	The port number for a secure browser login. The default is 9443.

For Example: To access a Video Session Recorder with an IP address of 192.168.0.100, using a secure browser login (https), enter:

https://192.168.0.100:9443

Note: 1. Valid entries for all of the Service Ports are from 1–65535.

2. Service ports cannot have the same value. You must set a different value for each one.

3. If there is no firewall (on an Intranet, for example), it doesn't matter what these numbers are set to, since they have no effect.

Archive Server

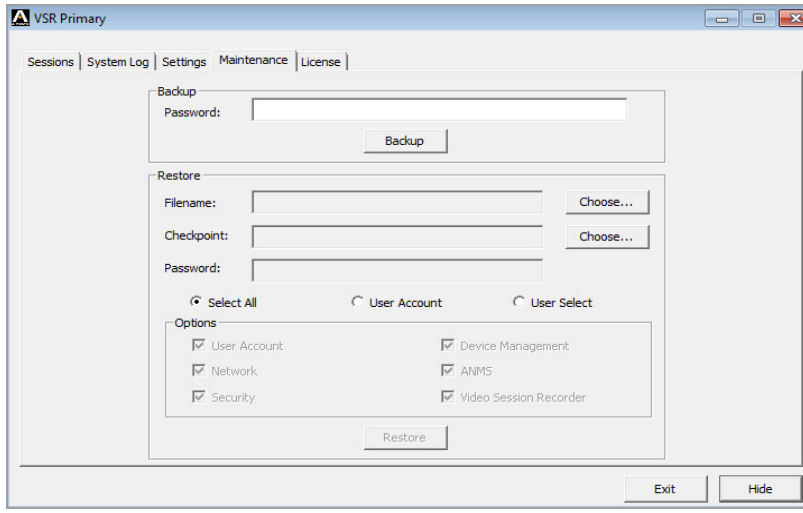
If you have installed a VSR Archive Server, input the IP Address and Port number of the computer hosting the software. For more information on configuring the Archive Server see *VSR Archive Server*, page 19, for details.

Disable Keystroke Recording

If you put a check in this box the Video Session Recorder will not record the keystrokes that occur on a computer during video sessions that are recorded (see page 41 for details).

Maintenance

The Maintenance tab is used to *Backup* and *Restore* system configuration settings and user account information to/from a file or system created *Checkpoint*. There are two sections:



Backup

To create a backup file, enter a password, then click *Backup* to save the file. Leave the *Password* field blank if you don't want to use a password. The saved data file contains the current system configuration and all user account information.

Restore

To restore data, click *Choose* to select a *Filename* or *Checkpoint* to restore a system created Checkpoint. Enter the *Password* if restoring from a file, and click **Restore**.

If using *Filename* to restore data, choose the type of data you want to restore:

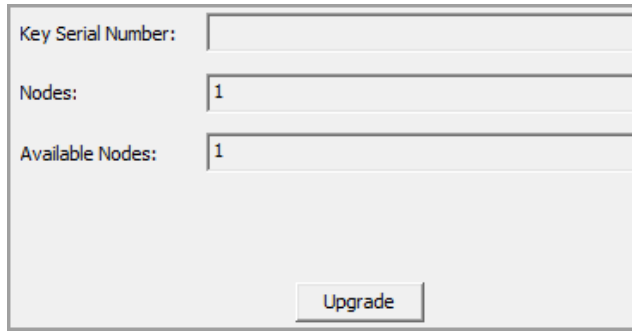
Select All: Restores all data from the backup file.

User Account: Restores only user account related data from the backup file.

User Select: Restores only the data (*User Account, Network, Security, Device Management, ANMS, and Video Session Recorder*) you select to recover.

License

The License tab is used to upgrade your software and add server licenses.



Upgrading the License

The license controls the total number of **Nodes** purchased and **Available Nodes** not in use; permitted with your Video Session Recorder installation. The license information is contained on the USB License Key that came with your purchase.

Upon completion of the VSR software installation, a default license for one primary server is automatically provided. To add more Video Session Recorder nodes, you must upgrade the license.

To upgrade the license:

1. Use the USB key that came with your package or contact your dealer to obtain a new license key for the number of primary and/or secondary servers you want to add.
2. Insert the license key into a USB port on your Video Session Recorder.
3. Login to the VSR application, and from the License tab click **Upgrade**.

You can now install and use additional Video Session Recorders (per the number of licenses purchased), which will communicate and work in conjunction over a network.

Note: 1. Once the upgrade has completed, it is no longer necessary to keep the key plugged into the USB port. Remove the key and place it somewhere safe, since you will need it for future upgrades.

2. If you lose the USB license key, contact your dealer to obtain another one. If you supply the key's serial number the new key will contain all of the information that was stored on the lost key.

Chapter 4
VSR Archive Server

Overview

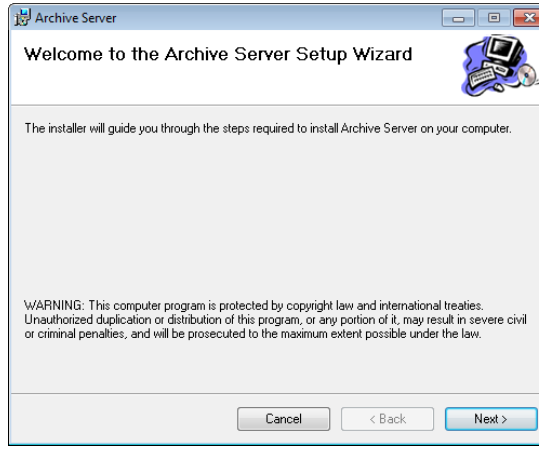
The VSR Archive Server allows you to store, playback, import, and export data created on VSR servers. The software automatically transfers a copy of the video log files from the Primary VSR server into an organized archive separate from the main system. This gives you the ability to purge older files from the main system but keep a safe archive of all videos for future use. The Archive Server runs in the background and updates the archive automatically every 15 minutes. To purchase this software, please see *Licenses*, page 4, for details.

Installing the VSR Archive Server

Starting the Installation

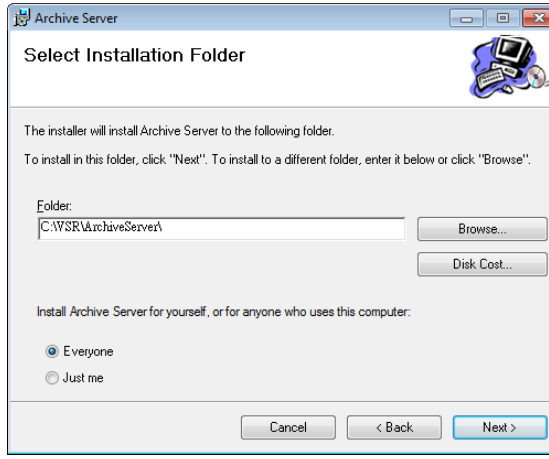
To install the Archive Server on a Windows system, insert the USB License Key into your computer, and do the following:

1. Put the software CD that came with your package into the computer's CD drive, or open the folder with the installation file.
2. Go to the folder where the *setup.exe* is located and double click it. A screen similar, to the one below, appears:


Archive Server
Welcome to the Archive Server Setup Wizard
The installer will guide you through the steps required to install Archive Server on your computer.
WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.
Cancel
< Back
Next >

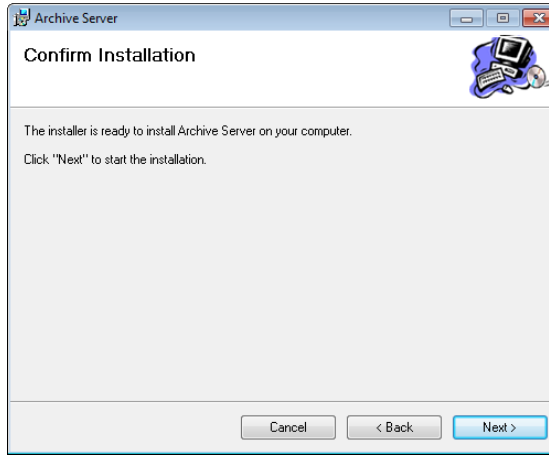
Click **Next** to continue.

3. On the *Select Installation Folder* page, specify the installation folder, or click **Browse** to choose the location where you want to install it. Then choose if you want to install it for yourself (**Just me**), or for anyone who uses this computer (**Everyone**). Click **Disk Cost** to view available drives and disk space.

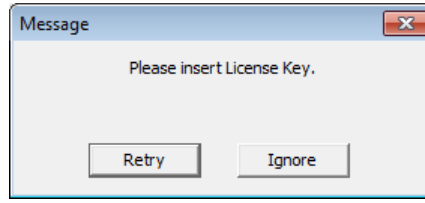

Archive Server
Select Installation Folder
The installer will install Archive Server to the following folder.
To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".
Folder:
C:\WSR\ArchiveServer\
Browse...
Disk Cost...
Install Archive Server for yourself, or for anyone who uses this computer:
Everyone
Just me
Cancel
< Back
Next >

Click **Next** to continue.

4. The *Confirm Installation* window appears, click **Next** to continue:

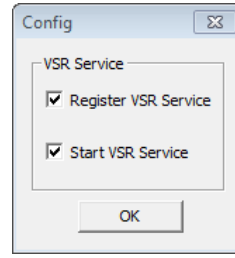

Archive Server
Confirm Installation
The installer is ready to install Archive Server on your computer.
Click "Next" to start the installation.
Cancel
< Back
Next >

5. If a message appears to insert the License Key, re-plug the USB License Key into your computer or try a different USB port, then click **Retry**.



Clicking **Ignore** will install the software but you will not be able to use it until the USB License Key has been made available.

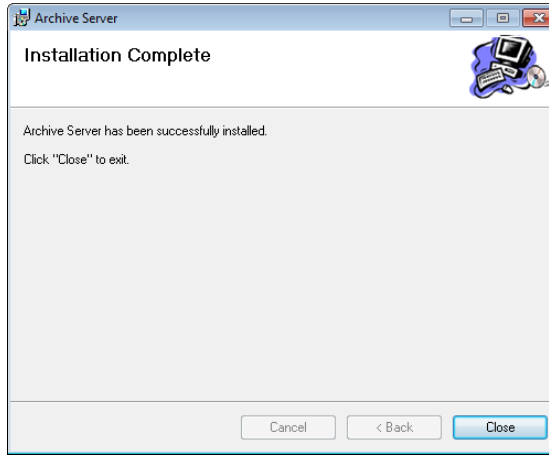
6. The **Config** dialog box appears, select the options and click **OK**:



Register VSR Service: This option registers the VSR Service with the Windows operating system so that it can run the software in the background.

Start VSR Service: This option will start the VSR Service automatically after the installation is complete. It is recommend to select both options.

7. When the installation is complete the following message will appear:

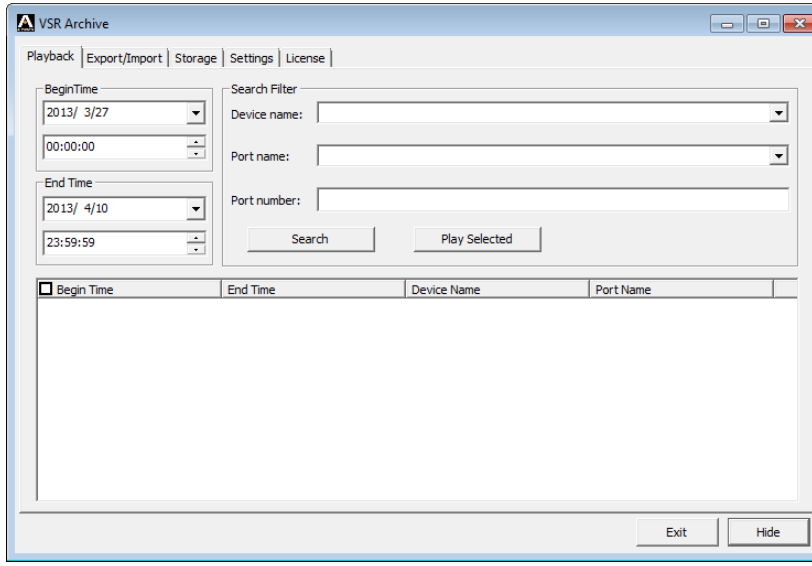


Licenses

Upon completion of the VSR software installation, a default license for one server is automatically provided. To add more Video Session Recorders, you must upgrade the license. To upgrade the license, See *License*, page 18, for details. For License options See *License Options*, page 5, for details.

Archive Server GUI

The Archive Server's interface has 5 tabs: *Playback*, *Export*/*Import*, *Storage*, *Settings*, and *License*; all described below. Once the software has been installed, double click the *Archive GUI* icon located on the desktop, and the *Playback* page appears:



Use the **Exit** button to shutdown the Archive Server, or **Hide** button to minimize the window to the task bar.

Setup

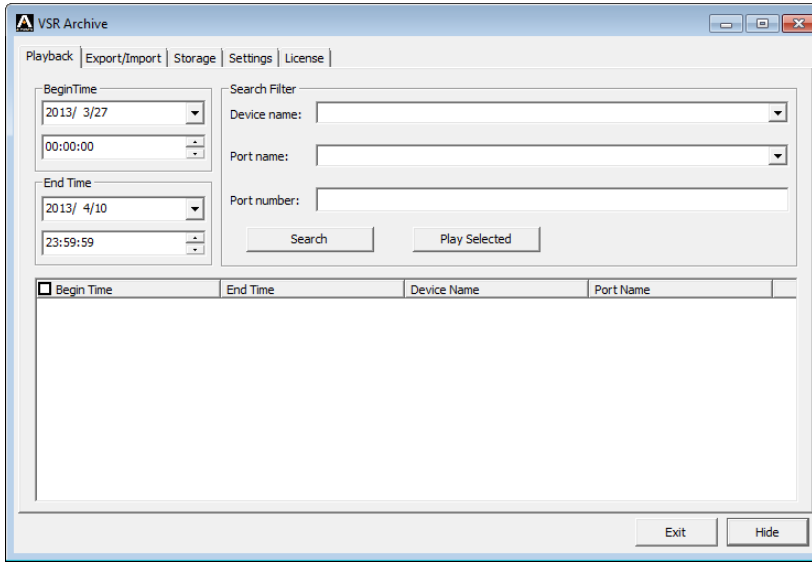
There are two steps to setup the Archive Server- set the Archive Server's IP address on the Primary VSR server, and add a storage location from the Archive Server's **Storage** tab.

First, configure the Archive Server's IP Address on the Primary VSR Server (see *Archive Server*, page 16). Next, add a storage location from the **Storage** tab (see *Storage*, page 28). The storage location is where the archived video log files are saved.

After the IP address is configured and a storage location is added, the Archive Server will begin to automatically archive all video log files created after the installation. The archive is updated every 15 minutes. To check for new video log files, go to the **Playback** tab and click *Search*. All new video log files will appear in the search window.

Playback

The *Playback* tab is used to search and playback video log files which have been archived or manually imported. To see a list of all video log files that have been archived, simply click the *Search* button.



The *Playback* tab has 3 sections used to search and playback archived video log files.

Begin Time/End Time

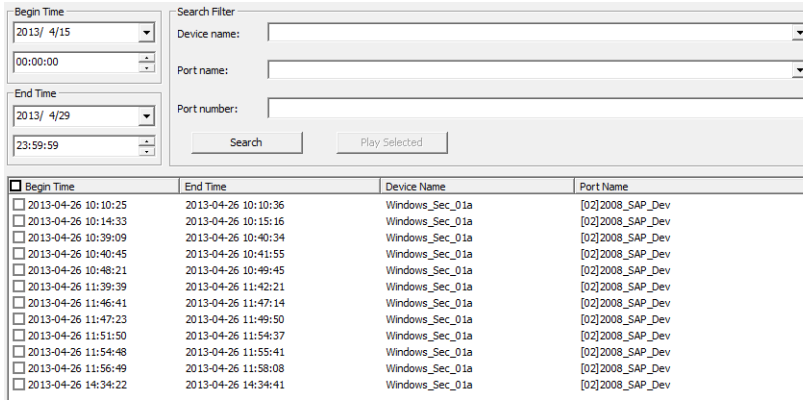
This section allows you to filter the search results by the begin and end time. The *Begin Time* and *End Time* refers to the time when the actual video log recording took place on the KVM switch.

Search Filter

The *Search Filter* is used to search for archived video log files by the *Port Name, Device Name*, or *Port Number* of the KVM switch they were recorded on. After inputting the search data, click **Search**. Your search results* will appear at the bottom of the page, and you can sort your results using the columns provided. If you would like to view all archived video logs, simply leave the fields blank and click **Search**.

Play Selected

To playback video logs, click **Search*** for a list of the archived video log to appear:



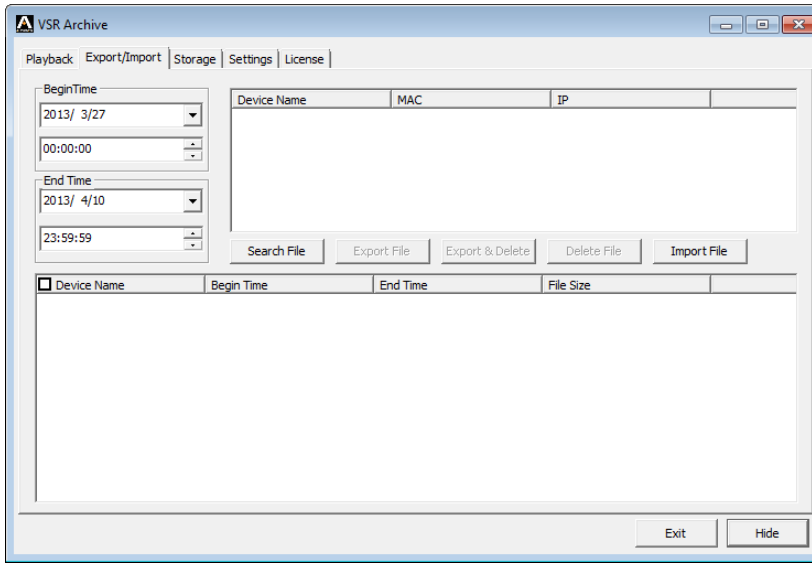
Select the checkboxes of the video(s) you want to playback, then click **Play Selected**. The video will open in a new window with the Video Log Viewer application. For information on the Video Log Viewer, see *Video Log Viewer*, page 39.

Note: 1. If no video log files appear after clicking *Search*, either the archive hasn't updated, in which case you should wait 15 minutes; or a storage location needs to be added on the **Storage** tab (see *Storage*, page 28).

2. Only video logs created after the Archive Server was installed are automatically archived from the Primary VSR server. Video logs created before the installation must be manually imported from the **Export/Import** tab (see *Export/Import*, page 26).

Export/Import

The *Export/Import* tab is used to export and import video log files in a single database (.vse) file format. The database (.vse) files can combine a large number of individual video logs into a single compressed file to reduce disk space, which can be exported for storage and imported for use. The Export/Import tab also allows you to import individual video log files (.dat) created on the VSR Primary Server.



You can search for files to export (which are already archived) by selecting a **Device Name** and clicking **Search File**; or manually import .vse or .dat files into the Archive Server by clicking **Import File**. For more information on imported files see *Import File* below.

Begin Time/End Time

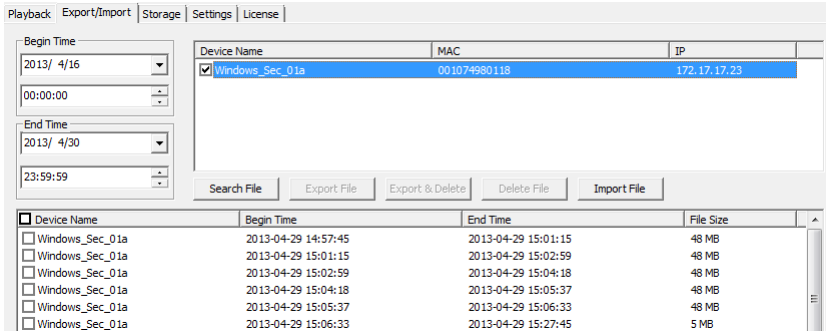
This section allows you to filter the search results by the begin and end time. The *Begin Time* and *End Time* refers to the time when the actual video recording took place on the KVM switch.

Device Name

This section lists the name(s) of the KVM switches which have been added to the Primary VSR server. You can select a device(s) and click Search for a list of individual video log files which have been archived from that KVM switch. After doing so you can select video logs to export into a .vse database file.

Search File

The *Search File* button is used to search for video log files on the **Device Name** you have selected. The results will appear in the lower section of the window, as shown below. After doing so you can select video logs to export into a .vse database file.



Export File

When you export logs they are saved in a single compressed .vse database file. Select the video log file(s) displayed in the lower window that you want to export, click **Export File** and provide a name to save the .vse file as.

Export & Delete

The *Export & Delete* button exports the selected files into a .vse database file and deletes the individual video log files that you are exporting from the Archive Server. This is a fast way to purge the individual files you are archiving into a single database.

Delete File

The *Delete File* button deletes the selected video log file from the Archive Server.

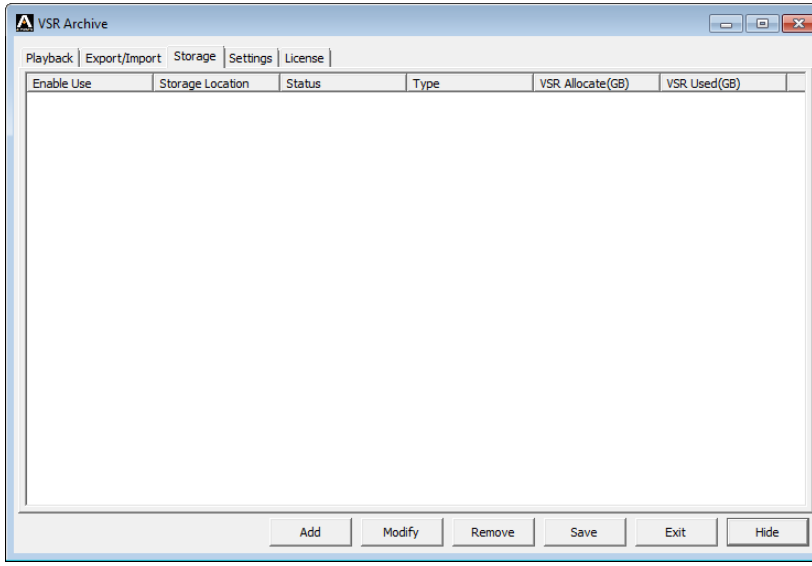
Import File

The *Import File* button is used to import database files (.vse) and individual video log files for viewing, archiving, or creating a new database- for export.

Click **Import File,** to browse and select the (.dat or .vse) file(s) to import, click **Open.** If you open a .vse database file: select the files from the list and click **Import**. Importing files will copy them into the Archive Server, therefore before you can import files, a storage location needs to be added from the **Storage** tab (see *Storage*, page 28). The storage location is where the archived files are saved, by the date they were created.

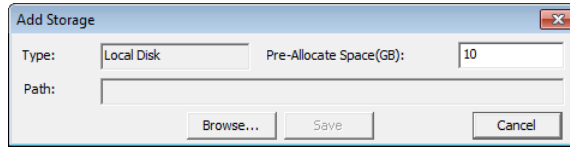
Storage

The *Storage* tab is used to add storage locations. This is where archived video logs are saved. You can add multiple storage locations for video logs. When the first location becomes full, the second will be used, and so on. Video logs are archived into folders according to the date they were created. The Archive Server cannot archive video logs until a storage location is **added** and **enabled**.



To add and enable a storage location, do the following:

1. Click **Add**, and the following window appears:

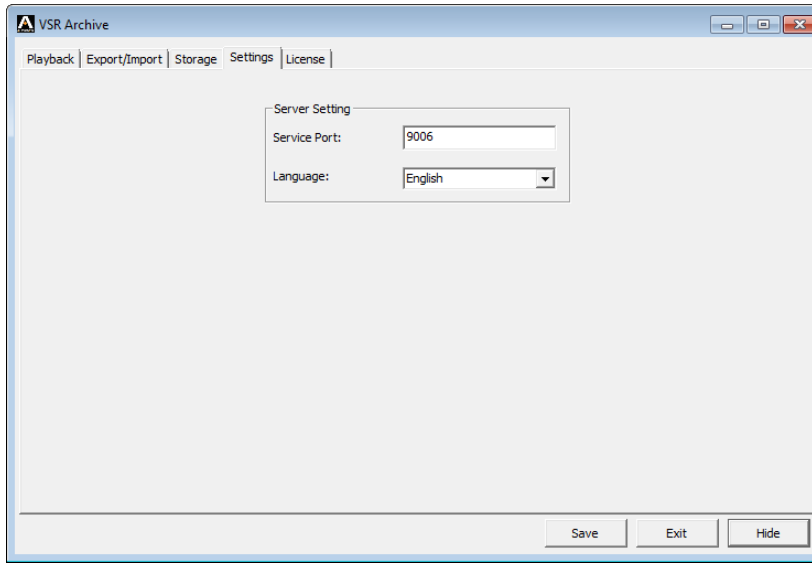


2. Type in the *Path* or click **Browse** to select a storage location.
3. In the *Pre-Allocate Space(GB)* field enter the maximum amount of disk space to use, then click **Save**. The storage location appears in the lower window.
4. Next, check the **Enable Use** box and click **Save**.

Select a Storage Location and click **Modify** to modify it, or **Remove** to remove it. Click **Save** to save the changes.

Settings

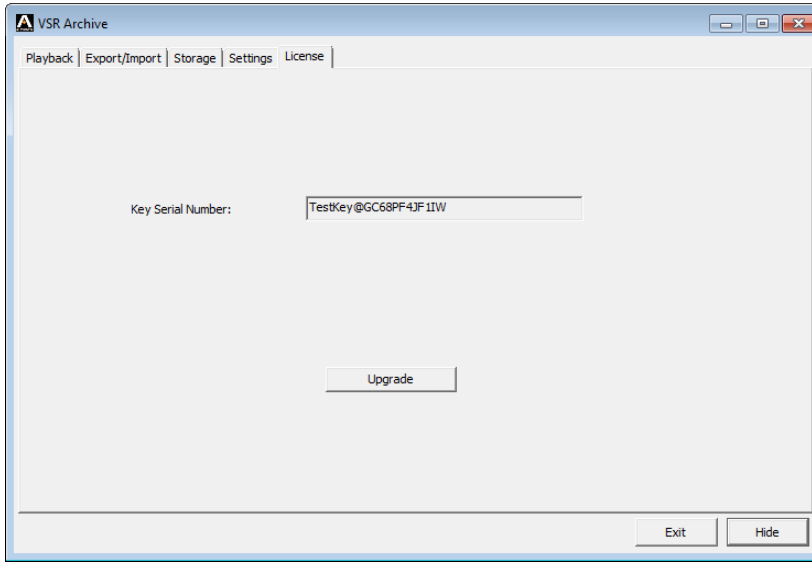
The Settings tab is used to set the Server Settings:



On this tab you can set the *Service Port* and *Language*. The default Service Port is **9006**.

License

Use the License tab to upgrade your license key. Insert the USB License Key into your computer, then click **Upgrade**.



If the upgrade fails, re-insert the USB License Key, or try a different USB port on your computer.

Chapter 5
The User Interface

Overview

The Video Session Recorder's user interface is accessed via web browser and contains the main features and functions. This chapter explains how to login to the Video Session Recorder and highlights the browser components.

Browser Login

The Video Session Recorder is accessed via an Internet browser running on any platform. To access the Video Session Recorder's browser interface, the VSR application must be started (See *VSR Application*, page 10, for details).

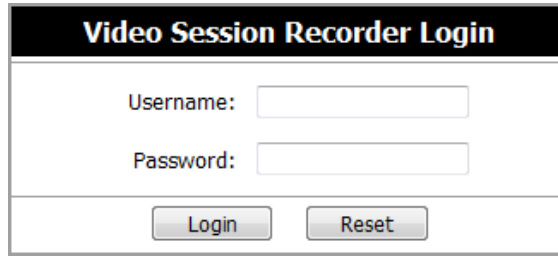
To access the Video Session Recorder, do the following:

1. Open the browser and specify the IP address and service port of the Video Session Recorder you want to access in the browser's location bar.

   For example: `https:\\192.168.0.100:9443`

2. When a Security *Alert* dialog box appears, accept the certificate – it can be trusted. If a second certificate appears, accept it as well (see *Trusted Certificates*, page 91).

Once you accept the certificate(s), the login page appears:

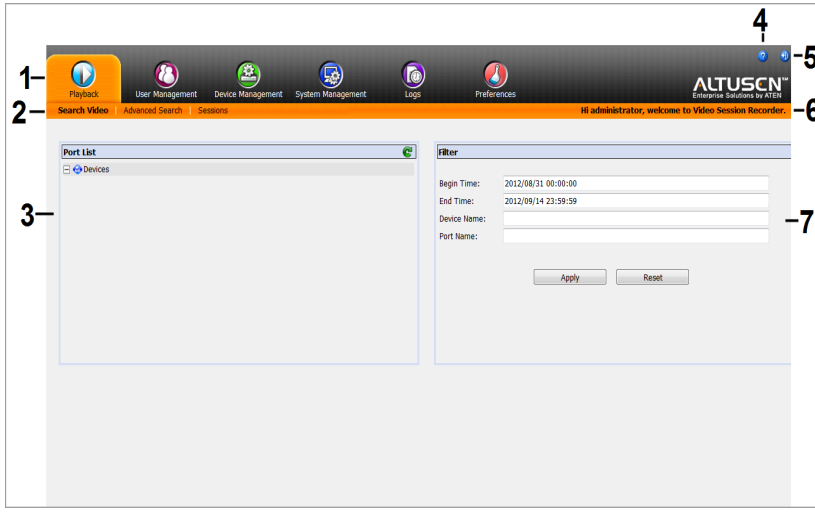


3. Provide your username and password, then click **Login** to bring up the Web Main Page.

Note: Since this is the first time you are logging in, use the default Username: *administrator*; and the default Password: *password*.

The Web Browser Main Page

Once users login and are authenticated, the *Web Browser Main Page* comes up, with the *Playback* page displayed:



Note: The screen depicts a Super Administrator's page. Depending on a user's type and permissions, not all of these elements appear.

Page Components

The web page screen components are described in the table, below:

No.	Item	Description
1	Tab Bar	The tab bar contains the Video Session Recorder's main operation categories. The items that appear in the tab bar are determined by the user's type, and the authorization options that were selected when the user's account was created.
2	Menu Bar	The menu bar contains operational sub-categories that pertain to the item selected in the tab bar. The items that appear in the menu bar are determined by the user's type, and the authorization options that were selected when the user's account was created.

No.	Item	Description
3	Sidebar	The Sidebar provides a tree view listing of components that relate to the various tab bar and menu bar selections. Clicking a component in the Sidebar brings up a page with the details that are relevant to it. **Note:** Some tabs don't have a sidebar as it's functions don't require one.
4	About	About provides information regarding the switch's current firmware version.
5	Logout	Click this button to log out of your Video Session Recorder's session.
6	Welcome Message	If this function is enabled a welcome message displays here.
7	Interactive Display Panel	This is your main work area. The screens that appears reflects your menu choices and Sidebar node selection.

The Tab Bar

The number and type of icons that appear on the Tab Bar at the top of the page are determined by the user's type (Super Administrator, Administrator, User) and the permissions assigned when the user's account was created. The functions associated with each of the icons are explained in the table below:

Icon	Function
	Playback: The Playback page is used to search and playback available video logs, and to monitor current browser sessions. Playback is discussed on page 35.
	User Management: The User Management page is used to create and manage Users and Groups. It can also be used to assign devices to them. This tab is available to the Super Administrator, as well as administrators and users who have been given User Management permission. The tab doesn't appear for other administrators and users. User Management is discussed on page 42
	Device Management: The Device Management page is used to add KVM devices and configure the ports for recording video logs. This page is available to the Super Administrator, as well as administrators and users who have been given Device Management permission. The tab doesn't appear for other administrators and users. The Device Management is discussed on page 58.
	System Management: The Systems Management page is used to configure the Video Session Recorder's system settings and to add secondary servers from the network. System Management is discussed on page 66.

Icon	Function
	Logs: The Log page displays the contents of the log file. The Log page is discussed on page 62.
	Preferences: The Preference page is used to customize the user's preferences for the user that is currently logged in. The Preferences page is discussed on page 84.

There are two small icons at the extreme right of the page. Their functions are described in the table, below:

Icon	Function
	Click this icon to bring up a panel with information about the Video Session Recorder firmware version.
	Click this icon to log out and end your Video Session Recorder session.

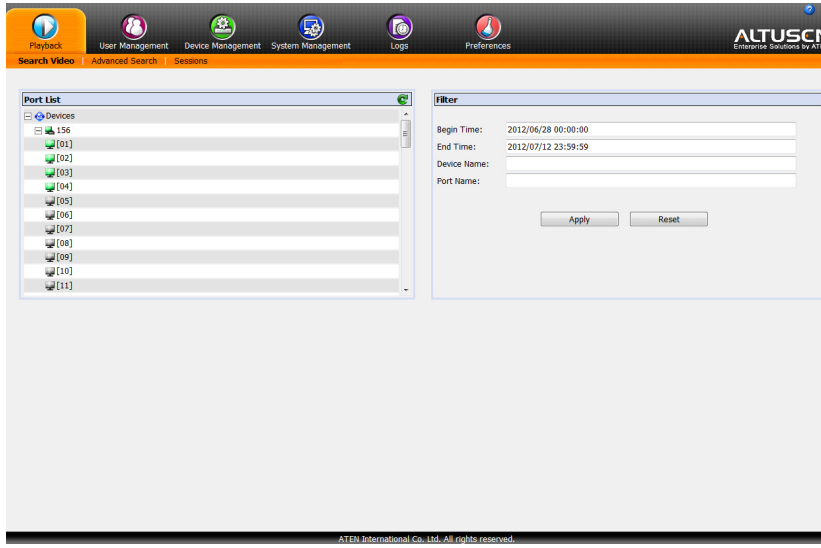
Chapter 6
Playback

Overview

The *Playback* tab is used to search and playback video log files and manage user sessions. The *Playback* tab has 3 menu pages; *Search Video*, *Advanced Search*, and *Sessions,* as described below. Before using the Playback tab, you must first add a KVM device, see *Recording KVM Ports*, page 58 for details.

Search Video

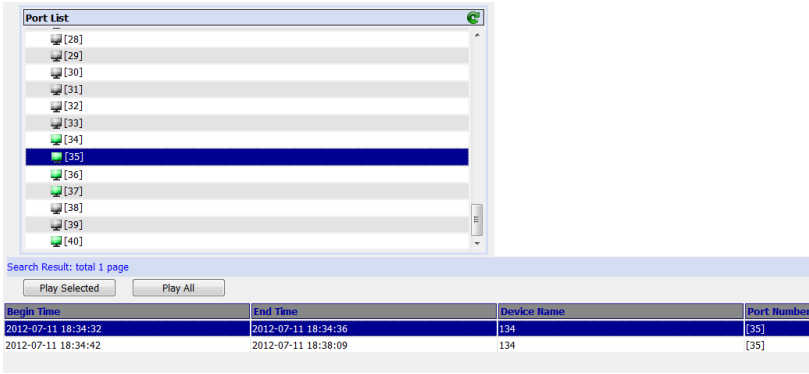
When you login to the Video Session Recorder the *Playback* tab comes up with the *Search Video* page displayed. The *Search Video* page is used to find video logs by device, port, or time.



The *Search Video* page is organized into several main areas. The *Port List* section shows all the KVM devices and ports that a user is permitted to access. The *Filter* section is used to filter the *Port List* to find videos within the chosen variables.

Port List

The *Port List* is used to find video logs by port. Ports list under the KVM device they are attached to. When you select a port with a video log, a section appears below it, listing all the video captured from that port, as shown here:

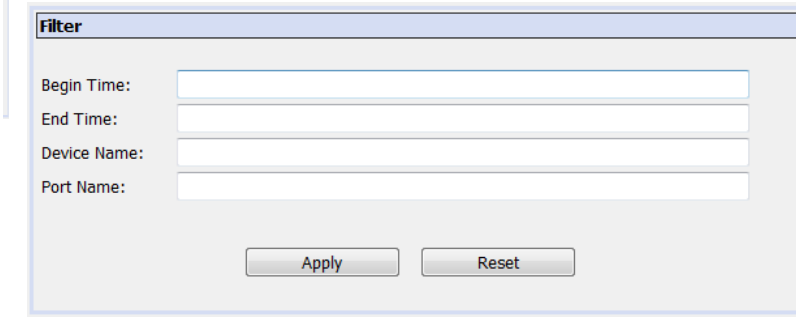


Playback

To playback a video log, select it from the *Search Result*s, then click *Play Selected*, or *Play All*. The video will open in a new window with the Video Log Viewer application. For information on the Video Log Viewer, see *Video Log Viewer*, page 39.

Filter

Use the *Filter* section to condense the *Port List* by *Begin Time, End Time, Port Name,* or *Device Name*. The *Begin Time* and *End Time* refers to when the recording took place.

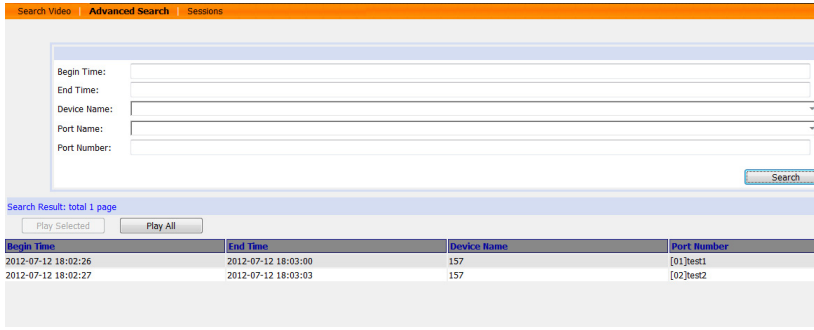


To filter the *Port List*, fill in the variables and click **Apply**.

To remove all filters click **Reset**.

Advanced Search

The *Advanced Search* page is used to search for video logs on a broad scale. You can search for video logs by *Begin Time, End Time, Port Name, Device Name*, or *Port Number*. The *Begin Time* and *End Time* refers to when the recording took place. After inputting your search data, click **Search**. Your search results will appear at the bottom of the page, as shown below:

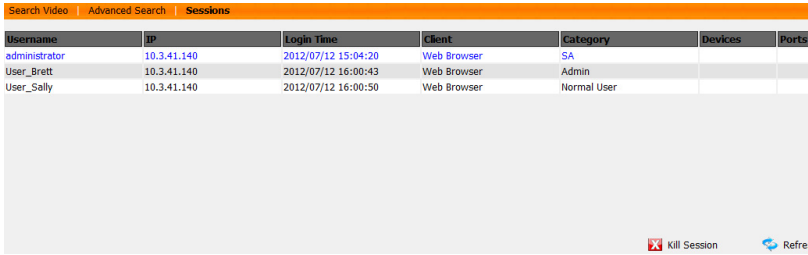


Playback

To playback a video log, select it from the *Search Result*s, then click *Play Selected*, or *Play All*. The video will open in a new window with the Video Log Viewer application. For information on the Video Log Viewer, see *Video Log Viewer*, page 39.

Sessions

The *Session* page lets the administrator and users with User Management permissions see at a glance which users are currently logged into the Video Session Recorder, and provides information about each of their sessions.



Note: 1. The Session page isn't available for ordinary users.

2. Users with User Management permissions can only see the sessions of ordinary users.

3. The *Category* heading lists the type of user who has logged in: SA (Super Administrator); Admin (Administrator); Normal user (User).

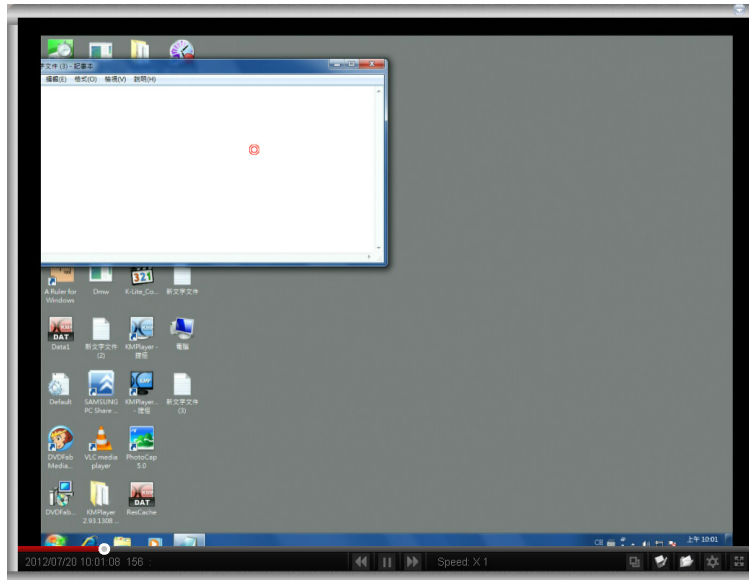
The meanings of the headings at the top of the page are fairly straightforward. The *IP* heading refers to the IP address that the user has logged in from; the *Login Time* refers to the user logged into the Video Session Recorder, and the *Device* and *Port* headings refer to the device and port a user is currently accessing.

- This page also gives the administrator the option of forcing a user logout by selecting the user and clicking *Kill Session* at the bottom of the page.
- The sort order of the information displayed can be changed by clicking the column headings.

Video Log Viewer

The *Video Log Viewer* is a build in video player that pops-up when executing video log files for playback. The Video Log Viewer is automatically used to view video logs from the Video Session Recorder's web sessions or directly from the directory where it was saved. The Video Log Viewer's playback tools are described below.

When you playback a video log, the *Video Log Viewer* pops-up, and a screen similar to this one appears:



Toolbar

The toolbar appears below the video and allows you to view information about the video and control playback features. The toolbar hides when no mouse movement is made for 3 seconds. To bring the toolbar into view simply move the mouse. The toolbar functions are described here:

Icon	Function
	Play: The *Play* button is used to resume playback of a video log that has been paused.
	Pause: The *Pause* button is used to stop playback of a video log that is being played.

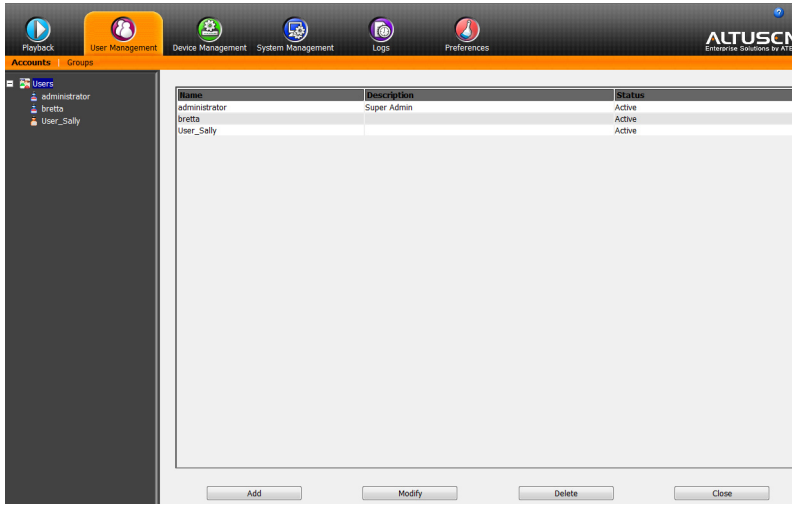
Icon	Function
	Faster: The *Faster* button is used to increase the playback speed of a video log. You can increase the speed X2, X4, or X8 of the normal playback rate.
	Slower: The *Slower* button is used to decrease the playback speed of a video log. You can decrease the speed 1/2, 1/4, or 1/8 of the normal playback rate.
	Progress Bar: The *Progress bar* shows how far along you are while viewing video logs. When viewing multiple video logs using the *Play All* feature, a solid red line on the progress bar represents the end of one video log, and the start of the next. Placing your mouse over any part of the Progress bar will produce a pop-up display of the time and date when the video log was captured, allowing you to quickly locate and go to reference points. You can click and drag the progress button forward or back to advance to any point of the video, or click anywhere on the progress bar to advance to a particular point.
	Resize Window: At the bottom right hand corner, you can click and drag the bar to resize the window. After doing so if the video doesn't fit within the resized window, you can scale the video using the *Scale Mode* feature (*see Scale Mode below).* **Note:** The entire window can be moved around the screen by holding a left click anywhere on the gray window frame, outside of the *Resize Window* area.
	Scale Mode: The *Scale Mode* icon allows you to change the video displays size in the Video Log Viewer's window. When you click the *Scale Mode* icon, three choices appear: ◆ *Keep Video Size:* Keeps the video display scaled at the original default size. ◆ *Keep Video Ratio*: Keeps the video display ratio scaled to fit within the resized window. ◆ *Scale Video to Window*: Scales the video display to the size of the entire window.
	Save Video: The *Save Video* icon allows you to save the current video log to a directory and encrypt it with a password. To save the video log, click **Save Video**, choose a directory, name the file, then click **Save**. After clicking *Save* the *Set Password* window will appear, enter a password for the video log file, or leave it blank for no password, then click **OK**. **Note:** Clicking *Cancel* at the *Set Password* prompt causes the save process to end and the file is not saved.
	Open Video: This icon is used to open previously saved video files. Click the icon, choose a video log file, then enter the password.

Icon	Function
	Control Panel: When playing videos, in addition to the video image, the *Control Panel* shows the operations (mouse clicks and key-strokes), username, and IP address of the person logged into the computer, arranged in order of time executed. If multiple people are logged into the KVM port, the *Control Panel* will display the users, and who conducts each operation. Click the icon to bring up the *Control Panel* window, and use the Pin icon located at the top left corner to hold/release the open window. The *User List* displays the users logged into the KVM port at the time the video log was recorded.
	Full Screen: This icon expands the Video Log Viewer window to fit the the entire screen. To exit *Full Screen* mode, click the *Full Screen* icon again.

Chapter 7
User Management

Overview

When you select the User Management tab the screen comes up with the Users page displayed:



The page is organized into two main areas: the Sidebar at the left, and the large main panel at the right.

- Users and groups appear in the panel at the left of the page. The large panel at the right provides more detailed information at-a-glance for each.
- There are separate menu bar entries for Accounts and Groups. Depending on the menu item selected, either Users or Groups are listed in the Sidebar.
- The sort order of the information displayed can be changed by clicking the main panel column headings.
- The buttons below the main panel are used to manage users and groups, as shown in the sections that follow.

Users

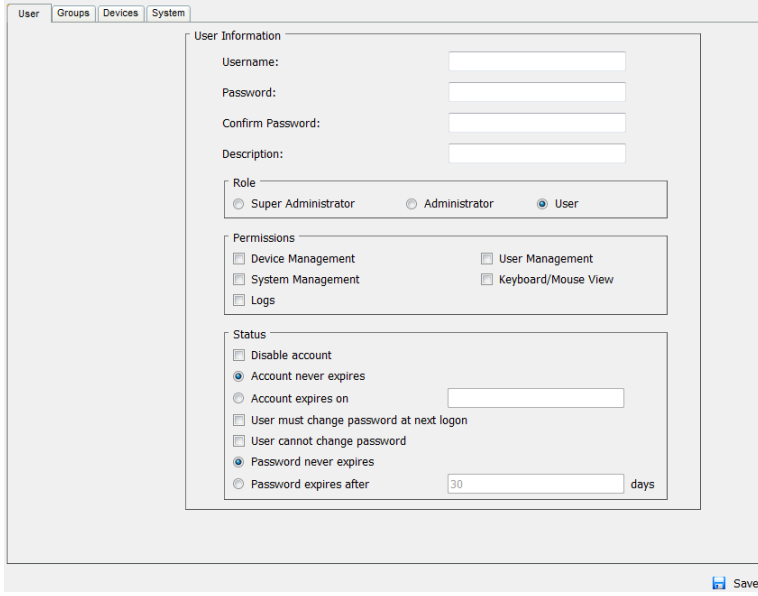
The Video Session Recorder supports three types of users, as shown in the table, below:

User Type	Role
Super Administrator	Access and manage ports and devices. Manage Users, and Groups. Configure the overall installation. Configure personal working environment.
Administrator	Access and manage authorized ports and devices. Manage Users and Groups. Configure personal working environment.
User	Access authorized ports and devices. Manage authorized ports and devices; configure personal working environment. **Note:** Users who have been given permission to do so, may also manage other users.

Adding Users

To add a user, and assign user permissions, do the following:

1. Select *Users* on the menu bar.
2. Click **Add** at the bottom of the main panel. The User notebook opens, with the *User* tab selected:



3. Enter the required information in the appropriate fields. A description of each of the fields is given in the table below:

Field	Description
Username	From 1 to16 characters are allowed depending on the Account Policy settings. see *Account Policy*, page 77.
Password	From 0 to 16 characters are allowed depending on the Account Policy settings. see *Account Policy*, page 77
Confirm Password	To be sure there is no mistake in the password, you are asked to enter it again. The two entries must match.
Description	Additional information about the user that you may wish to include.
Role	There are three categories: Super Administrator, Administrator and User. There is no limitation on the number of accounts that can be created in each category. ◆ The Super Administrator is responsible for the overall installation configuration and log maintenance; user management; and device and system management. The Super Administrator's permissions (see page 45) are automatically assigned by the system and cannot be altered. ◆ The default permissions for Administrators include everything except Keyboard/Mouse View, but the permissions can be altered for each Administrator by checking or un-checking any of the permissions checkboxes. ◆ The default permissions for Users include no permissions, but the permissions can be altered for each User by checking or un-checking any of the permissions checkboxes. **Note:** Users who have been given User Management privileges cannot access or configure Groups.

Field	Description
Permissions **Note:** For ordinary users, in addition to enabling Device Management, the user must also be given those rights for each device that he will be allowed to manage. (See *Device Assignment*, page 54 for details).	◆ Enabling *Device Management* allows a user to view the settings and devices on the Device Management tab (see *Device Management*, page 58). ◆ Enabling *User Management* allows a user to create, modify, and delete user and group accounts. ◆ Enabling *Log* allows a user to access the system log (see *Logs*, page 62 for details) ◆ Enabling *System Management* allows a user to access and configure settings in the System Management tab. ◆ Enabling *Keyboard/Mouse View* allows the user to use the Control Panel feature from within the Video Log Viewer, which allows you to view the detailed log of keyboard and mouse operations (mouse clicks, key-strokes), see page 41 for details.
Status	Status allows you to control the user's account and access to the installation, as follows: ◆ *Disable Account* lets you suspend a user's account without actually deleting it, so that it can be easily reinstated in the future. ◆ If you don't want to limit the time scope of the account, select *Account never expires*; if you do want to limit the amount of time that the account remains in effect, select *Account expires on*, and key in the expiration date. ◆ To make a password permanent, so that the user cannot change it to something else, select *User cannot change password*. ◆ For security purposes, administrators may want users to change their passwords from time to time. ◆ If not, select *Password never expires*. This allows users to keep their current passwords for as long as they like. ◆ If so, select *Password expires after*, and key in the number of days allowed before the password expires. Once the time is up, a new password must be set.

4. At this point you can assign the new user to a group by selecting the *Groups* tab – the Groups page is discussed on page 50, or you can assign the user's device access rights by selecting the *Devices* tab – the Devices page is discussed on page 54, or you can assign VSR configuration rights by selecting the *System* tab – the System page is discussed on page 56.
5. When your selections have been made click **Save**.
6. When the Operation Succeeded message appears, click **OK**.

7. Click **Users** in the Sidebar to return to the main screen. The new user appears in the Sidebar list and in the main panel, as well.
   - The Sidebar *Users* list can expand and collapse. If the list is expanded, click the minus symbol (–) next to the Users icon to collapse it; if it is collapsed there is a plus symbol (+) next to the icon. Click the plus symbol to expand it.
   - The icon for super Administrators has two red bands; the icon for Administrators has one black band.
   - The large main panel shows the user's name; the description that was given when the account was created; and whether the account is currently active or has been disabled.

Modifying User Accounts

To modify a user account, do the following:

1. In the Sidebar *User* list, click the user's name.

   – or –

   In the main panel, select the user's name.

2. Click **Modify**.
3. In the *User* page that comes up, make your changes, then click **Save**.

Note: The User page is discussed on page 43; the Groups page is discussed on page 50, the Devices page is discussed on page 54.

Deleting User Accounts

To delete a user account, do the following:

1. In the main panel, select the user's name.
2. Click **Delete**.
3. Click **OK**.

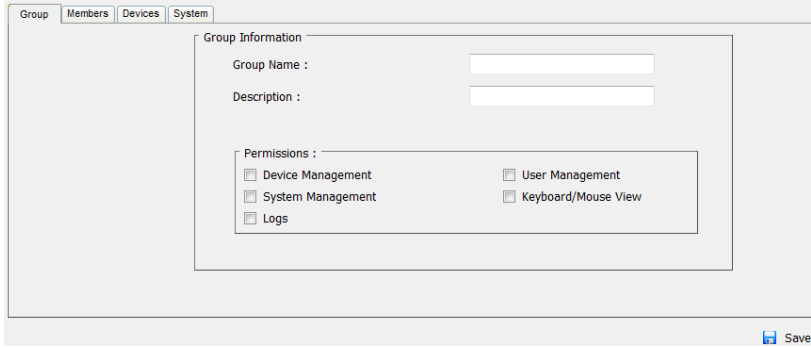
Groups

Groups allow administrators to easily and efficiently manage users and devices. Since device access rights apply to anyone who is a member of the group, administrators need only set them once for the group, instead of having to set them for each user individually. Multiple groups can be defined to allow some users access to specific devices, while restricting other users from accessing them.

Creating Groups

To Create a group, do the following:

1. Select *Groups* on the menu bar.
2. Click **Add** at the bottom of the main panel. The Group notebook opens, with the *Group* tab selected:



3. Enter the required information in the appropriate fields. A description of each of the fields is given in the table below:

Field	Description
Group Name	A maximum of 16 characters is allowed.
Description	Additional information about the user that you may wish to include. A maximum of 63 characters is allowed.
Permissions	Permissions and restrictions for groups are set by checking the appropriate boxes. These are the same permissions as the ones specified for Users. See *Permissions*, page 47 for details.

4. At this point you can assign users to the group by selecting the Members tab – the Members page is discussed on page 52, or you can assign the

group's device access rights by selecting the Devices tab – the Devices page is discussed on page 54, or you can assign VSR configuration rights by selecting the System tab – the System page is discussed on page 56.

5. When your selections have been made click **Save**.
6. When the *Operation Succeeded* message appears, click **OK**.
7. Click **Group** in the Sidebar to return to the main screen. The new group appears in the Sidebar Group list and in the main panel.
   - The Sidebar *Group* list can expand and collapse. If the list is expanded, click the minus symbol (–) next to the *Users* icon to collapse it; if it is collapsed there is a plus symbol (+) next to the icon. Click the plus symbol to expand it.
   - The large main panel shows the group's name, and the description that was given when the group was created (the *Status* column is inactive).

Note: You must perform Step 7 before attempting to add a new group, or else the new group you are creating will replace the group you just finished creating.

Modifying Groups

To modify a group, do the following:

1. In the Sidebar Group list, click the group's name.

   – or –

   In the main panel, select the group's name.
2. Click **Modify**.
3. Click **OK**.
4. In the *Group* notebook that comes up, make your changes, then click **Save**.

Note: The *Group* page is discussed on page 47; the *Members* page is discussed on page 52, The *Devices* page is discussed on page 54, and the *System* page is discussed on page 56.

Deleting Groups

To delete a group, do the following:

1. In the Sidebar, click the *Groups* icon.
2. In the main panel, select the group's name.
3. Click **Delete**.
4. Click **OK**.

Users and Groups

There are two ways to manage users and groups: from the Users notebook; and from the Group notebook.

Note: Before you can assign users to groups, you must first create them. See *Adding Users*, page 43

Assigning Users to a Group From the User's Notebook

To assign a user to a group from the User's notebook, do the following:

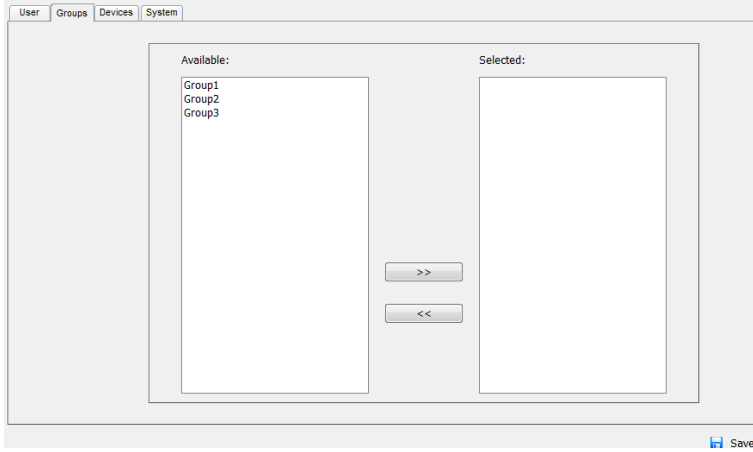
1. In the Sidebar *User* list, click the user's name.

   – or –

   In the main panel, select the user's name.

2. Click **Modify**.

3. In the *User* notebook that comes up, select the *Groups* tab. A screen, similar to the one below, appears:



4. In the *Available* column, select the group that you want the user to be in.

5. Click the **Right Arrow** to put the group's name into the Selected column.

6. Repeat the above for any other groups that you want the user to be in.

7. Click **Save** when you are done.

Note: If a user has permissions in addition to the ones assigned to the group, the user keeps those permissions in addition to the group ones.

Removing Users From a Group From the User's Notebook

To remove a user from a group from the User's notebook, do the following:

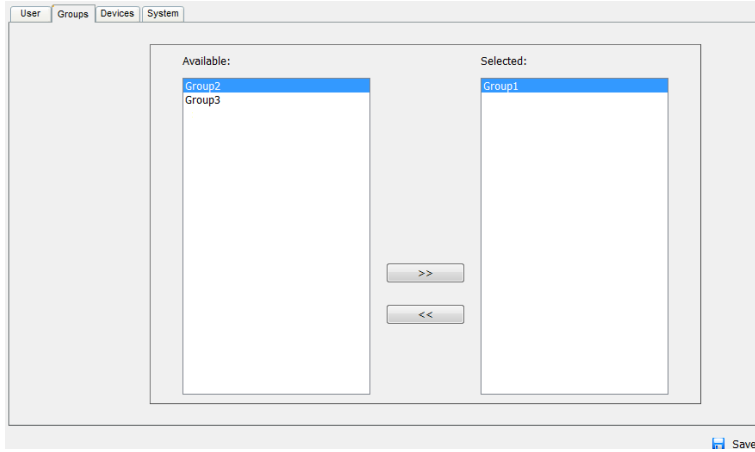
1. In the Sidebar *User* list, click the user's name.

   – or –

   In the main panel, select the user's name.

2. Click **Modify**.

3. In the *User* notebook that comes up, select the Groups tab. A screen, similar to the one below, appears:



4. In the *Selected* column, select the group that you want to remove the user from.

5. Click the **Left Arrow** to remove the group's name from the *Selected* column. (It goes back into the *Available* column.)

6. Repeat the above for any other groups that you want to remove the user from.

7. Click **Save** when you are done.

Assigning Users to a Group From the Group's Notebook

To assign a user to a group from the Group notebook, do the following:

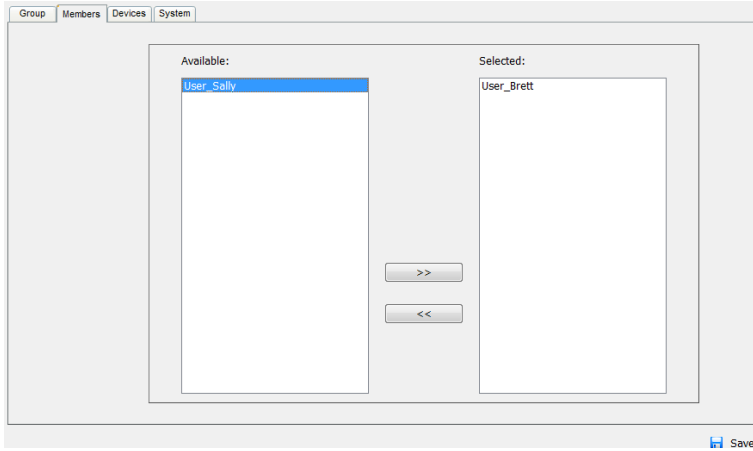
1. In the Sidebar *Group* list, click the group's name.

   – or –

   In the main panel, select the group's name.

2. Click **Modify**.

3. In the *Group* notebook that comes up, select the *Members* tab. A screen, similar to the one below, appears:



4. In the *Available* column, select the user that you want to be a member of the group.

5. Click the **Right Arrow** to put the user's name into the *Selected* column.

6. Repeat the above for any other users that you want to be members of the group.

7. Click **Save** when you are done.

Note: If a user has permissions in addition to the ones assigned to the group, the user keeps those permissions in addition to the group ones.

Removing Users From a Group From the Group's Notebook

To remove a user from a group from the Group's notebook, do the following:

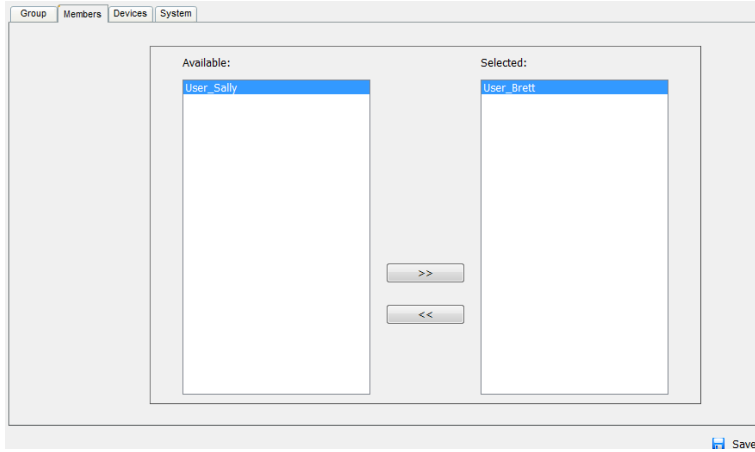
1. In the Sidebar *Group* list, click the group's name

   – or –

   In the main panel, select the group's name.

2. Click **Modify**.

3. In the *Group* notebook that comes up, select the *Members* tab. A screen, similar to the one below, appears:



4. In the *Selected* column, select the user that you want to remove from the group.

5. Click the **Left Arrow** to remove the user's name from the *Selected* column. (It goes back into the *Available* column.)

6. Repeat the above for any other users that you want to remove from the group.

7. Click **Save** when you are done.

Device Assignment

When a user logs in to the Video Session Recorder, the interface comes up with the *Playback* page displayed. All the ports that the user is permitted to access are listed in the Port List at the left of the page. Access permissions for ports and the devices connected to them are assigned on a port-by-port basis from the User or Group list on the Sidebar of the User Management page.

Assigning Device Permissions From the User's Notebook

To assign device permissions to a user from the *User's* notebook, do the following:

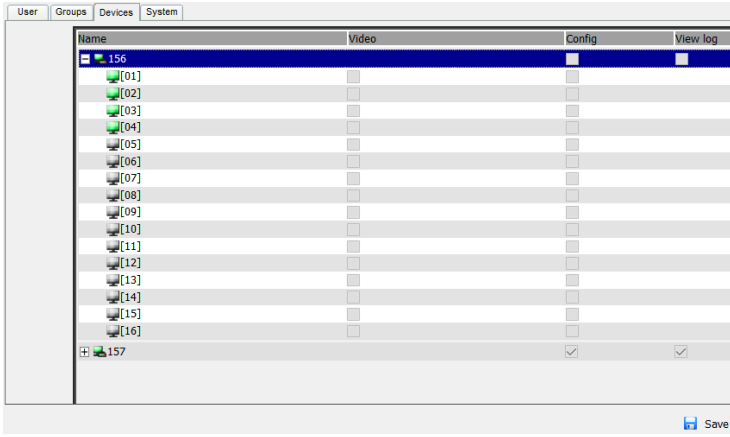
1. In the Sidebar *User* list, click the user's name.

   – or –

   In the main panel, select the user's name.

2. Click **Modify**.

3. In the *User* notebook that comes up, select the *Devices* tab. A screen, similar to the one below, appears:



4. Make your permission settings for each port according to the information provided below:

   Name: Each port accessible to the user is listed under the Names column.

   Video: Selecting this checkbox gives a user the ability to search and view video logs for a port.

Config: Selecting this checkbox gives a user the ability to enable/ disable ports for devices found in the Device Management tab. Permissions are applied from the top down, therefore you must select a KVM device in order for the individual ports below it to be available for access.

View Log: Selecting this checkbox allows a user the ability to view system logs for a KVM device from the *Logs* tab.

5. When you have finished making your choices, click **Save**.
6. In the confirmation popup that appears, click **OK**.

Assigning Device Permissions From the Group's Notebook

To assign device permissions to a Group of users, do the following:

1. In the Sidebar *Groups* list, click the group's name.

   – or –

   In the main panel, select the group's name.
2. Click **Modify**.
3. In the *Groups* notebook that comes up, select the *Devices* tab.
4. The screen that comes up is the same one that appears in the User's notebook. The only difference is that whatever settings you make apply to all members of the group instead of just one individual member.

   Make your device assignments according to the information described under *Assigning Device Permissions From the User's Notebook*, page 54.

System Permissions

Systems permissions allows administrators to give users or groups the ability to make systems configuration changes from the System Management tab.

Assigning System Permissions From the User's Notebook

To assign systems configuration permissions to a user from the *User's* notebook, do the following:

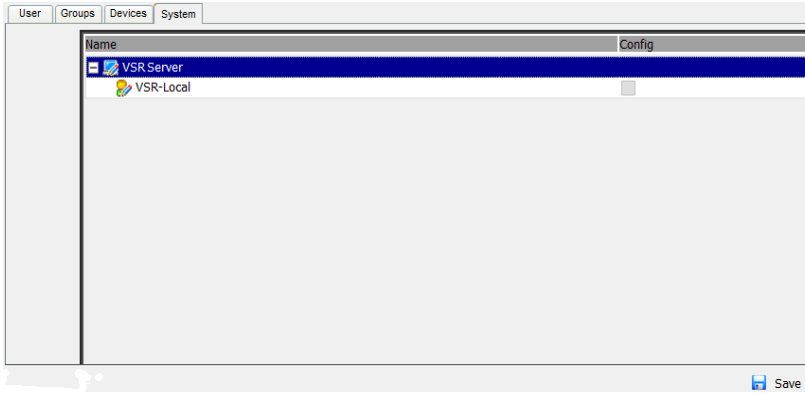
1. In the Sidebar *User* list, click the user's name.

   – or –

   In the main panel, select the user's name.

2. Click **Modify**.

3. In the *User* notebook that comes up, select the *System* tab. A screen, similar to the one below, appears:



4. Select the Video Session Recorder (VSR) you want to allow System Configuration changes on.

5. Click the **Config** checkbox.

6. Click **Save**.

Assigning System Permissions From the Group's Notebook

To assign systems configuration permissions to a user from the *Group's* notebook, do the following:

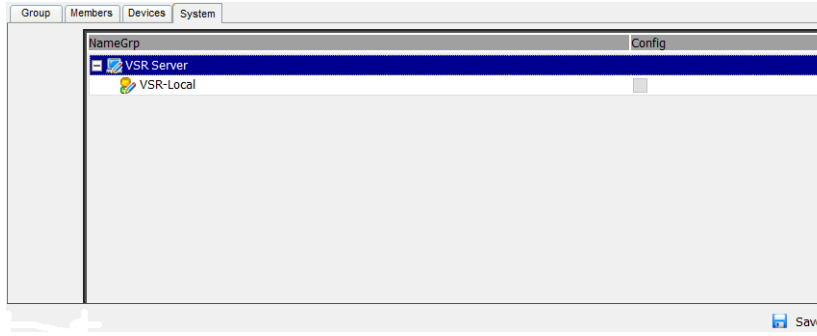
1. In the Sidebar *Groups* list, click the group's name.

   – or –

   In the main panel, select the group's name.

2. Click **Modify**.

3. In the *Group* notebook that comes up, select the *System* tab. A screen, similar to the one below, appears:



4. Select the Video Session Recorder (VSR) you want to allow System Configuration changes on.

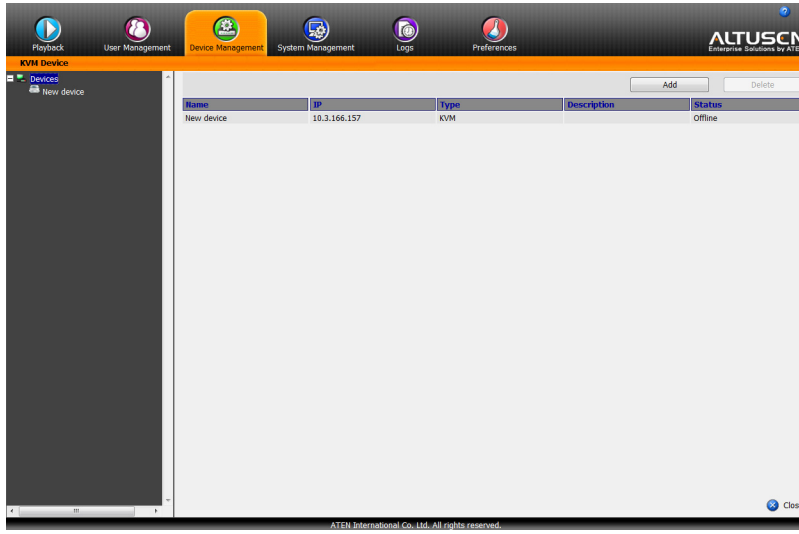
5. Click the **Config** checkbox.

6. Click **Save**.

Chapter 8
Device Management

Overview

The purpose of the Device Management tab is to add KVM devices and configure ports through which the Video Session Recorder can record video logs. The Device Management tab opens with *Devices* selected in the Sidebar, and the main page showing a list of KVM devices which have been added:



Recording KVM Ports

To record video logs you must add a KVM switch, then enable the switch and/or ports on the KVM's *Device Settings* page. Enabled ports are recorded by the Video Session Recorder every time they are accessed through the KVM switch, and are saved as a video log file. Logs are viewed from the *Playback* tab. There is no limit to the number of KVM devices that you can add or ports you can enable. The Video Session Recorder can simultaneously record a maximum of 12 ports at one time, across multiple KVM devices.

Adding KVM Devices

To add a KVM switch to the *KVM Device* list, do the following:

1. From the *Device Management* page, click **Add**.

   A pop-up window appears:

2. Fill in the IP address and Service Port number of the KVM switch you are adding, and click **Add**.
3. The KVM switch will appear in the *Devices* list on the sidebar, and on the *Device Management* main page.

Note: 1. After adding a KVM switch check to be sure the *Status* column of the KVM device is *Online*.

2. An *Offline* status indicates the KVM device can't be reached over the network. Check that the IP address and Service Port numbers are correct, and that the KVM switch is online.

Enabling KVM Devices

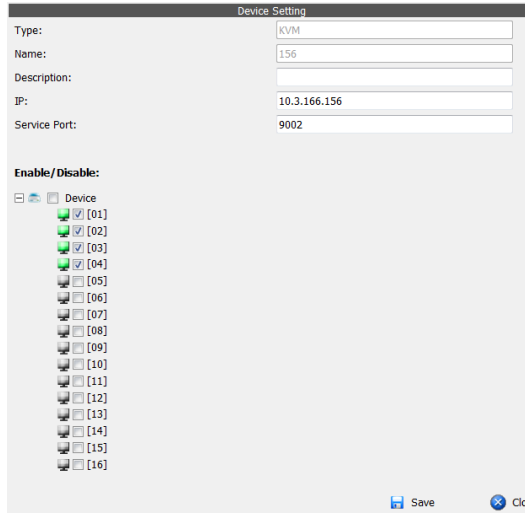
To enable the KVM switch to record video sessions, do the following:

1. In the sidebar *Devices* list, click the KVM device name.
2. Under **Enable/Disable** put a check in the *Device* box.
3. The KVM switch will now record video sessions anytime a port on the KVM switch is accessed. To enable/disable individual ports, see *Configuring KVM Ports* on the next page.

Configuring KVM Ports

To enable a *KVM Port*, so that the Video Session Recorder records it when accessed through the switch, do the following:

1. In the sidebar *Devices* list, click the KVM device name.
2. The KVM's *Devices Settings* page appears:



3. Enable the ports that you want the Video Session Recorder to record by checking the boxes. Video Logs will be created every time the enabled ports are accessed through the KVM switch.
4. After configuring the KVM's Device Settings, click **Save**.

A description of the *Device Settings* fields are given in the table below.

Field	Explanation
Type	Describes the switch device type for your reference.
Name	Provides the name of the KVM switch for your reference.
Description	Enter information about the KVM device that you want to include.
IP	Enter the IP address of the KVM switch here.
Service Port	Enter the service port number of the KVM switch here.
Enable/Disable	Checking a box enables the port, so that when it is accessed through the KVM switch, a video log is recorded. If a port or device's checkbox is not selected, it is disabled, and no video logs will be recorded for that port. You can enable all ports by selecting the KVM *Device's* checkbox, or individual ports by selecting each port you want to enable.

Deleting KVM Devices

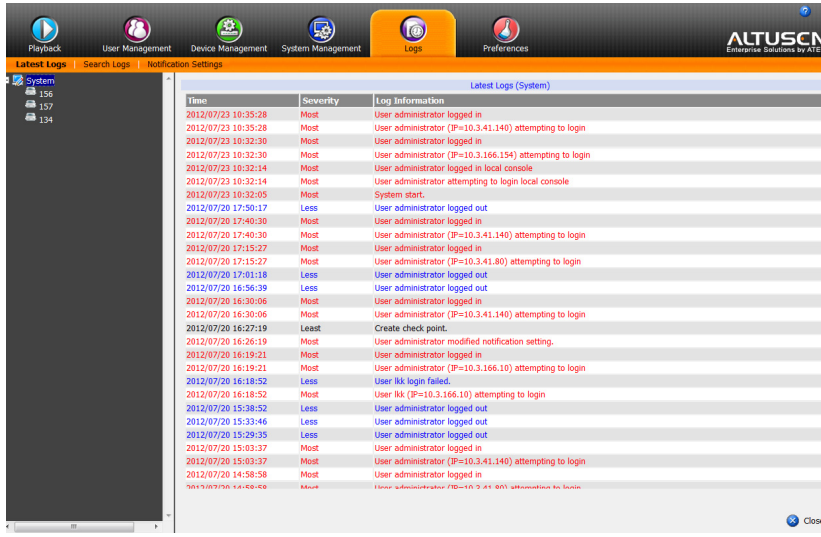
To delete a KVM Switch from the *KVM Device* list, do the following:

1. In the main panel, select the KVM device you want to delete.
2. Click **Delete**.

Chapter 9
Logs

Overview

The Video Session Recorder logs all the events that take place on it. To view the contents of the log, click the *Log* tab. The *Latest Logs* page, similar to the one below, appears:


Playback
User Management
Device Management
System Management
Logs
Preferences
ALTUSEN
Enterprise Solutions by ATEN
Latest Logs
Search Logs
Notification Settings
System
156
157
134
Latest Logs (System)
Time
Severity
Log Information
2012/07/23 10:35:28 Most User administrator logged in
2012/07/23 10:35:28 Most User administrator (IP=10.3.41.140) attempting to login
2012/07/23 10:32:30 Most User administrator logged in
2012/07/23 10:32:30 Most User administrator (IP=10.3.166.154) attempting to login
2012/07/23 10:32:14 Most User administrator logged in local console
2012/07/23 10:32:14 Most User administrator attempting to login local console
2012/07/23 10:32:05 Most System start.
2012/07/20 17:50:17 Less User administrator logged out
2012/07/20 17:40:30 Most User administrator logged in
2012/07/20 17:40:30 Most User administrator (IP=10.3.41.140) attempting to login
2012/07/20 17:15:27 Most User administrator logged in
2012/07/20 17:15:27 Most User administrator (IP=10.3.41.80) attempting to login
2012/07/20 17:01:18 Less User administrator logged out
2012/07/20 16:56:39 Less User administrator logged out
2012/07/20 16:30:06 Most User administrator logged in
2012/07/20 16:30:06 Most User administrator (IP=10.3.41.140) attempting to login
2012/07/20 16:27:19 Least Create check point.
2012/07/20 16:26:19 Most User administrator modified notification setting.
2012/07/20 16:19:21 Most User administrator logged in
2012/07/20 16:19:21 Most User administrator (IP=10.3.166.10) attempting to login
2012/07/20 16:18:52 Less User lkk login failed.
2012/07/20 16:18:52 Most User lkk (IP=10.3.166.10) attempting to login
2012/07/20 15:38:52 Less User administrator logged out
2012/07/20 15:33:46 Less User administrator logged out
2012/07/20 15:29:35 Less User administrator logged out
2012/07/20 15:03:37 Most User administrator logged in
2012/07/20 15:03:37 Most User administrator (IP=10.3.41.140) attempting to login
2012/07/20 14:58:58 Most User administrator logged in
Close

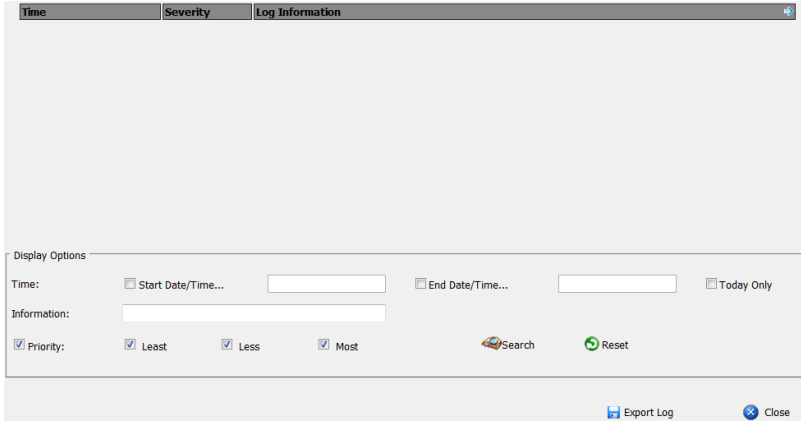
Latest Logs

The *Latest Logs* page displays events that take place on the Video Session Recorder, and provides a breakdown of the time, severity, user, and a description of each event.

The log file tracks a maximum of 512 events. When the limit is reached, the oldest events get discarded as new events come in. You can filter the event logs by *System*, or KVM device by selecting either from the sidebar tree list.

Search Logs

The *Search Logs* page allows you to search logs by *Time*, *Information*, and *Priority*. In addition, you can export your search into a custom log file. When you click *Search Logs* from the menu bar, the following screen appears:



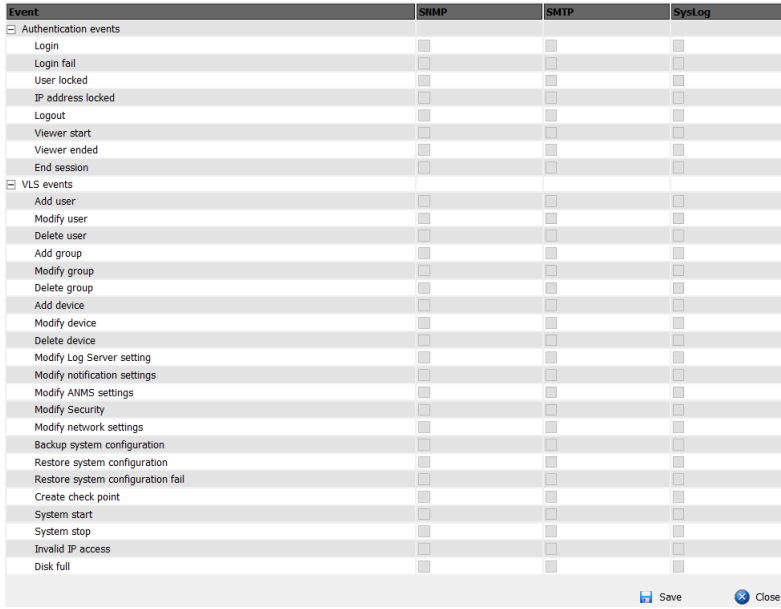
The purpose of the fields found at the bottom of the search page are described in the following table:

Field	Explanation
Time	This feature lets you search for events that occurred at specific times, as follows: **Today Only:** Only the events for the current day are displayed. **Start Date/Time:** Searches for events from a specific date and time to the present. After checking **Start Date/Time**, click inside the text box in order to bring up the calendar. When you have made your calendar choices, click the **A** icon at the lower right of the calendar panel. Set the date and time that you want the search to start from. All events from the Start date/time to the present are displayed. **End Date/Time:** Searches for events from a specific date and time to a specific date and time. First select the Start Date/Time (described above); check **End Date/Time** to set the ending date and time. After checking End Date/Time, click inside the text box in order to bring up the calendar. When you have made your calendar choices, click the **A** icon at the lower right of the calendar panel.

Field	Explanation
Information	Searches for a particular word or string. Key the word or string into the *Information* text box. Only events containing that word or string are displayed. Wildcards (? for single characters; * for multiple characters) and the keyword **or** are supported. E.g., h*ds would return hands and hoods; h?nd would return hand and hind, but not hard; h*ds or h*ks would return hands and hooks.
Priority	Searches based on the severity rating of the event. *Least* events appear in black; *Less* events appear in blue; *Most* events appear in red. First put a check in the *Priority* checkbox; then check the severity options you want to search for (you can check more than one item). Only events that match the severity ratings you specified appear in the display.
Search	Click to apply the filter choices.
Reset	Click this button to clear the entries in the dialog box and start with a clean slate.
Export Log	Clicking *Export Log* will bring up window giving you the option to Save or Open the search log as a *.csv file.

Notification Settings

The *Notification Settings* page lets you decide which events trigger a notification, and how the notifications are sent out:



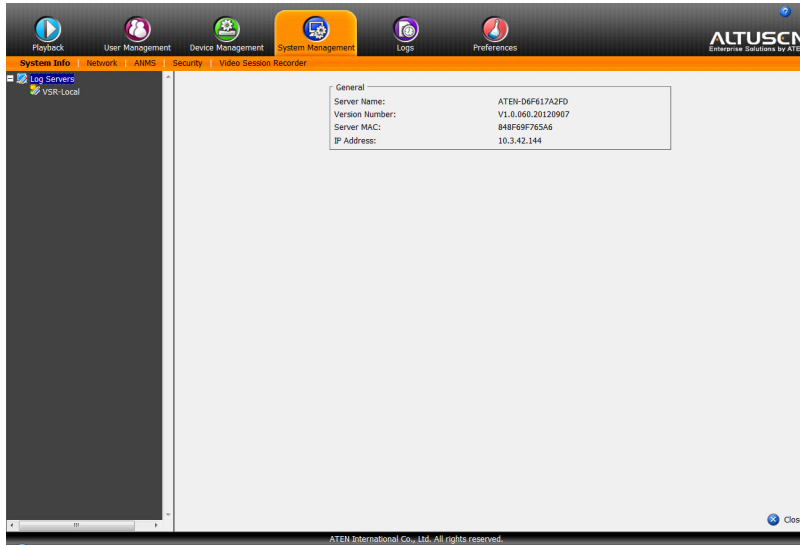
Notifications can be sent via SNMP trap, SMTP email, written to the SysLog file, or any combination of the three. A check mark (√) indicates that notification of the event is permitted for the method specified in the column heading; an empty box indicates that notification is not restricted.

Note: In any of the columns, you can use Shift-Click or Ctrl-Click to select a group of events. Clicking to permit/restrict any one of them causes all of them to change in unison.

Chapter 10
System Management

Overview

The Systems Management tab is used to view and manage the Video Session Recorder's system settings. When you select the *System Management* tab the screen comes up with the *System Info* page displayed:

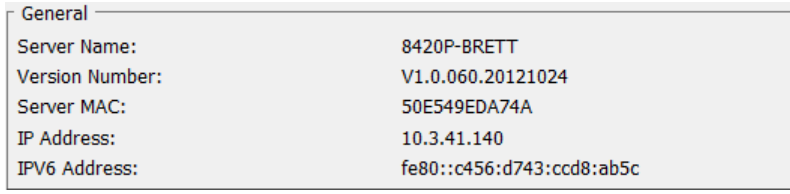


The page is organized into two main areas: the Sidebar at the left, and the large main panel at the right.

- The *Log Servers* list appears in the panel at the left of the page. The large panel at the right provides detailed information about the menu or sidebar selection
- There are separate menu bar options selecting *Log Servers* or a Video Session Recorder from the sidebar list
- With *Log Servers* selected you will see *System Info, Network, ANMS,* and *Security* on the menu bar.
- When a Video Session Recorder is selected from the sidebar, it's *Log Server Settings* page appears.

System Info

When you select the *System Management* tab the *System Info* page appears with *General* information about the local Video Session Recorder, as shown and described below:



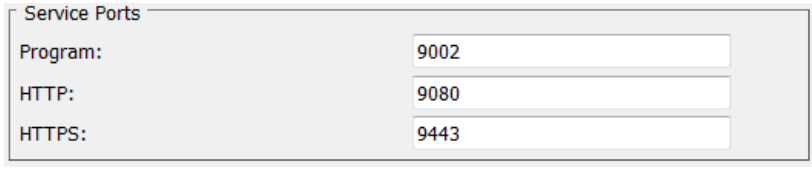
Item	Meaning
Server Name	Displays the computer name of the server hosting the Video Session Recorder application.
Version Number	Displays the Video Session Recorder's firmware version.
Server MAC	Displays the MAC address of the computer hosting the Video Session Recorder application.
IP Address	Displays the Video Session Recorder's IP address.
IPV6 Address	Displays the Video Session Recorder's IPV6 address.

VSR-Local

The *VSR-Local* device found on the sidebar is the system settings page for the local Video Session Recorder. Selecting this device allows you to configure the settings for *IP Address*, *Name*, *Description*, and local *VSR Space* for saving video session files. For more information on these settings see *Log Servers*, page 83 for details.

Network

The *Network* page is used to specify the service ports used to access the Video Session Recorder, as shown here:



As a security measure, if a firewall is being used, the Administrator can specify the port numbers that the firewall will allow. If a port other than the default is used, users must specify the port number as part of the IP address when they log in. If an invalid port number (or no port number) is specified, the Video Session Recorder will not be found. An explanation of the fields is given in the table below:

Field	Explanation
Program	This is the port number to connect a computer running the VSR application as a *Secondary Server*, to a Video Log *Primary Server*. The default is 9002.
HTTP	The port number for a browser login. The default is 9080.
HTTPS	The port number for a secure browser login. The default is 9443.

For Example: To access the Video Session Recorder with an IP address of 192.168.0.100, using a secure browser login (https), enter:

https://192.168.0.100:9443

Note: 1. Valid entries for all of the Service Ports are from 1–65535.

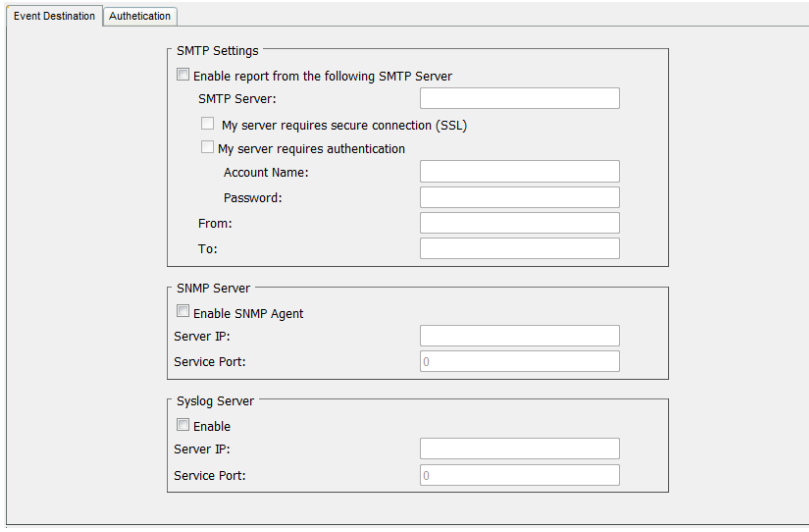
2. Service ports cannot have the same value. You must set a different value for each one.

3. If there is no firewall (on an Intranet, for example), it doesn't matter what these numbers are set to, since they have no effect.

ANMS

The ANMS (Advanced Network Management Settings) page is used to set up login authentication and authorization management from external sources. It is organized as a notebook with two tabs – each with a series of related panels, as described, below:

Event Destination



- SMTP Settings

  To have the Video Session Recorder email reports from the SMTP server to you, do the following:

  1. Enable the *Enable report from the following SMTP server*, and key in either the IPv4 address, IPv6 address, or domain name of the SMTP server.
  2. If your server requires a secure SSL connection, put a check in the *My server requires secure connection (SSL)* checkbox.
  3. If your server requires authentication, put a check in the *My server requires authentication* checkbox, and key in the appropriate account information in the *Account Name* and *Password* fields.

4. Key in the email address of where the report is being sent from in the *From* field.

Note:
1. Only one email address is allowed in the *From* field, and it cannot exceed 64 Bytes.
2. 1 Byte = 1 English alphanumeric character.

5. Key in the email address (addresses) of where you want the SMTP reports sent to in the *To* field.

Note: If you are sending the report to more than one email address, separate the addresses with a semicolon. The total cannot exceed 256 Bytes.

- SNMP Server

  To be notified of SNMP trap events, do the following:

  1. Check Enable *SNMP Agent*.
  2. Key in either the IPv4 address, IPv6 address, or domain name of the computer to be notified of SNMP trap events.
  3. Key in the port number. The valid port range is 1–65535.

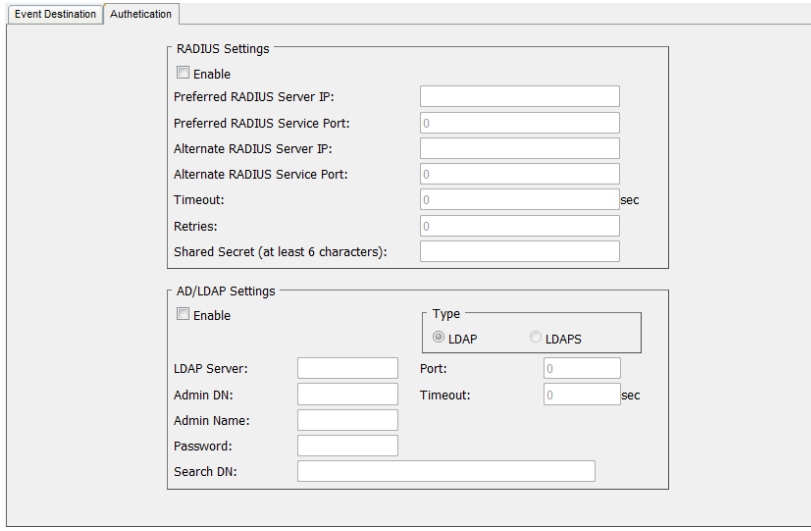
  Note: The logs that are notified of SNMP trap events are configured on the Notification Settings page under the *Log* tab. See *Notification Settings*, page 65 for details**.**

- Syslog Server

  To record all the events that take place on the Video Session Recorder and write them to a Syslog server, do the following:

  1. Check **Enable**.
  2. Key in either the IPv4 address, IPv6 address, or domain name of the Syslog server.
  3. Key in the port number. The valid port range is 1-65535.

Authentication



- Disable Local Authentication

  Selecting this option disables login authentication on the Video Session Recorder. The server can only be accessed using LDAP, LDAPS, MS Active Directory, or RADIUS authentication.

- RADIUS Settings

  To allow authentication and authorization for the Video Session Recorder through a RADIUS server, do the following:

  1. Check **Enable**.
  2. Fill in the IP addresses and service port numbers for the *Preferred* and *Alternate* RADIUS servers. You can use the IPv4 address, the IPv6 address or the domain name in the IP fields.
  3. In the *Timeout* field, set the time in seconds that the Video Session Recorder waits for a RADIUS server reply before it times out.
  4. In the *Retries* field, set the number of allowed RADIUS retries.
  5. In the *Shared Secret* field, key in the character string that you want to use for authentication between the Video Session Recorder and the RADIUS Server. A minimum of 6 characters is required.

6. On the RADIUS server, Users can be authenticated with any of the following methods:
   - Set the entry for the user as **su/xxxx**

     Where *xxxx* represents the Username given to the user when the account was created on the Video Session Recorder.
   - Use the same Username on both the RADIUS server and the Video Session Recorder.
   - Use the same Group name on both the RADIUS server and the Video Session Recorder.
   - Use the same Username/Group name on both the RADIUS server and the Video Session Recorder.

   In each case, the user's access rights are the ones assigned that were assigned when the User of Group was created on the Video Session Recorder. (See *Adding Users*, page 43.)

- LDAP / LDAPS Authentication and Authorization Settings

  To allow authentication and authorization for the Video Session Recorder via LDAP / LDAPS, refer to the information in the table, below:

Item	Action
Enable	Put a check in the Enable checkbox to allow LDAP / LDAPS authentication and authorization.
Type	Click a radio button to specify whether to use LDAP or LDAPS.
LDAP Server IP and Port	Fill in the IP address and port number for the LDAP or LDAPS server. ◆ You can use the IPv4 address, the IPv6 address or the domain name in the LDAP Server field. ◆ For LDAP, the default port number is 389; for LDAPS, the default port number is 636.
Admin DN	Consult the LDAP / LDAPS administrator to ascertain the appropriate entry for this field. For example, the entry might look like this: ou=kn4132,dc=aten,dc=com
Admin Name	Key in the LDAP administrator's username.
Password	Key in the LDAP administrator's password.
Search DN	Set the distinguished name of the search base. This is the domain name where the search starts for user names.
Timeout	Set the time in seconds that the Video Session Recorder waits for an LDAP or LDAPS server reply before it times out.

On the LDAP / LDAPS server, Users can be authenticated with any of the following methods:

- With MS Active Directory schema.

  Note: If this method is used, the LDAP schema for MS Active Directory must be extended.See *LDAP Server Configuration*, page 71, for details.

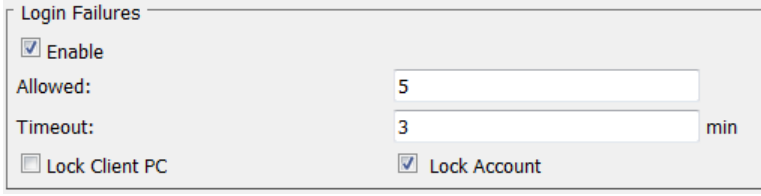
- Without schema – Only the Usernames used on the Video Session Recorder are matched to the names on the LDAP / LDAPS server. User privileges are the same as the ones configured on the switch.
- Without schema – Only Groups in AD are matched. User privileges are the ones configured for the groups he belongs to on the switch.
- Without schema – Usernames and Groups in AD are matched. User privileges are the ones configured for the User and the Groups he belongs to on the switch.

Security

The Security page is divided into 5 panels, as described in the sections that follow.

Login Failures

For increased security, the Login Failures section allows administrators to set policies governing what happens when a user fails to log in successfully.

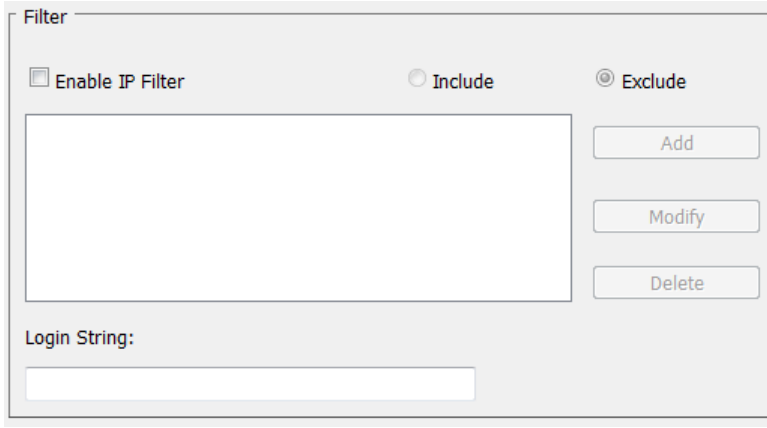


To set the Login Failures policy, check the *Enable* checkbox (the default is for Login Failures to be enabled). The meanings of the entries are explained below.

Entry	Explanation
Allowed	Sets the number of consecutive failed login attempts that are permitted from a remote computer. The default is 5 times.
Timeout	Sets the amount of time a remote computer must wait before attempting to login again after it has exceeded the number of allowed failures. The default is 3 minutes.
Lock Client PC	If this is enabled, after the allowed number of failures have been exceeded, the computer attempting to log in is automatically locked out. No logins from that computer will be accepted. The default is enabled. **Note:** This function relates to the client computer's IP. If the IP is changed, the computer will no longer be locked out.
Lock Account	If this is enabled, after the allowed number of failures have been exceeded, the user attempting to log in is automatically locked out. No logins from the username and password that have failed will be accepted. The default is enabled.

Note: If Login Failures is not enabled, users can attempt to log in an unlimited number of times with no restrictions. For security purposes, we recommend that you enable this function and enable the lockout policies.

Filter



- IP Filtering

  IP Filters control access to the Video Session Recorder based on the IP addresses of the client computers attempting to connect. A maximum of 100 IP filters are allowed. If any filters have been configured, they appear in the IP Filter list box.

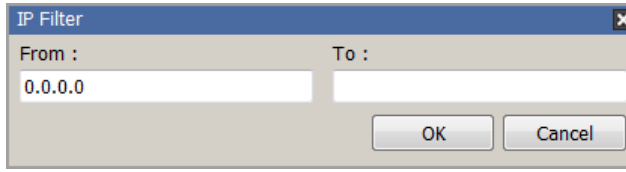
  To enable IP filtering, **Click** to put a check mark in the *IP Filter Enable* checkbox.

  - If the include button is checked, all the addresses within the filter range are allowed access; all other addresses are denied access.
  - If the exclude button is checked, all the addresses within the filter range are denied access; all other addresses are allowed access.

- Adding Filters

  To add an IP filter, do the following:

  1. Click **Add**. A dialog box similar to the one below appears:



  2. Key the address you want to filter in the *From*: field.
  3. Key in the end number of the range in the *To*: field.
     - To filter a single IP address, key the same address in both the From and To fields.
  4. After filling in the address, click **OK**.
  5. Repeat these steps for any additional IP addresses you want to filter.

- Modifying Filters

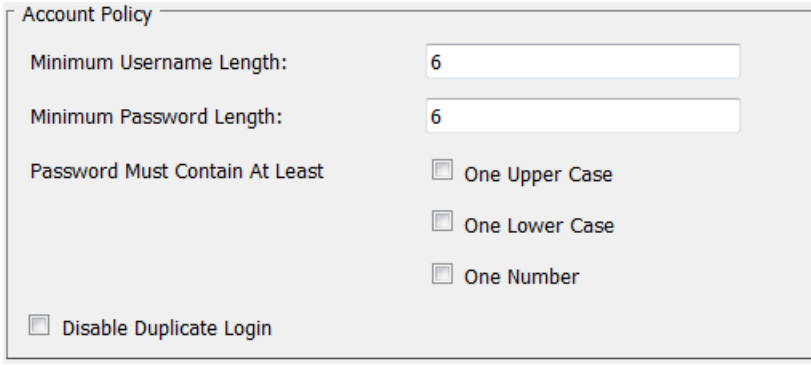
  To modify a filter, select it in the IP Filter list and click **Modify**. The Modify dialog box is similar to the Add dialog box. When it comes up, simply delete the old address(es) and replace it with the new one(s).

- Deleting Filters

  To delete a filter, select it in the IP Filter list and click Delete.

Account Policy

In the Account Policy section, system administrators can set policies governing usernames and passwords.

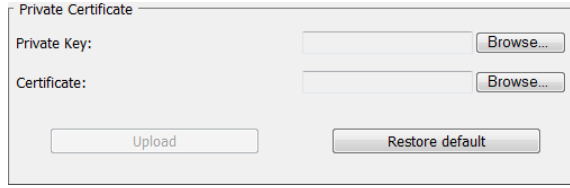


The meanings of the Account Policy entries are explained in the table below:

Entry	Explanation
Minimum Username Length	Sets the minimum number of characters required for a username. Acceptable values are from 1–16. The default is 6.
Minimum Password Length	Sets the minimum number of characters required for a password. Acceptable values are from 0–16. A setting of 0 means that no password is required. Users can login with only a Username. The default is 6.
Password Must Contain At Least	Checking any of these items requires users to include at least one uppercase letter, one lowercase letter or one number in their password. **Note:** This policy only affects user accounts created after this policy has been enabled, and password changes to existing user accounts. Users accounts created before this policy was enabled, with no change to the existing password, are not affected.
Disable Duplicate Login	Check this to prevent users from logging in with the same account at the same time.

Private Certificate

When logging in over a secure (SSL) connection, a signed certificate is used to verify that the user is logging in to the intended site. For enhanced security, the *Private Certificate* section allows you to use your own private encryption key and signed certificate, rather than the default ATEN certificate.



There are two methods for establishing your private certificate: generating a self-signed certificate; and importing a third-party certificate authority (CA) signed certificate.

- Generating a Self-Signed Certificate

  If you wish to create your own self-signed certificate, a free utility – openssl.exe – is available for download over the web. See *Self-Signed Private Certificates*, page 92 for details about using OpenSSL to generate your own private key and SSL certificate.

- Obtaining a CA Signed SSL Server Certificate

  For the greatest security, we recommend using a third party certificate authority (CA) signed certificate. To obtain a third party signed certificate, go to a CA (Certificate Authority) website to apply for an SSL certificate. After the CA sends you the certificate and private encryption key, save them to a convenient location on your computer.

- Importing the Private Certificate

  To import the private certificate, do the following:

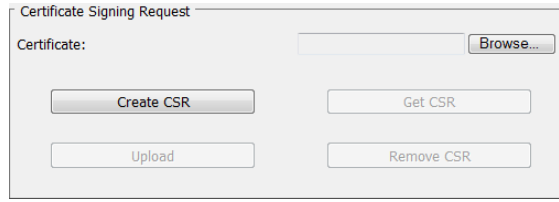
1. Click **Browse** to the right of *Private Key*; browse to where your private encryption key file is located; and select it.
2. Click **Browse** to the right of *Certificate*; browse to where your certificate file is located; and select it.
3. Click **Upload** to complete the procedure.

Note: 1. Clicking **Restore Default** returns the device to using the default ATEN certificate.

2. Both the private encryption key and the signed certificate must be imported at the same time.

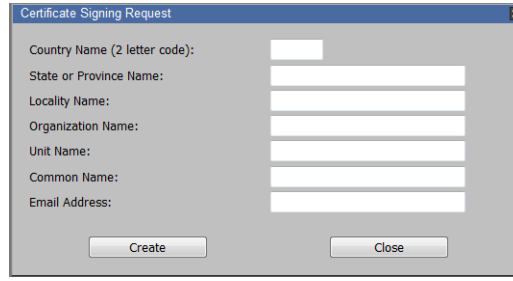
Certificate Signing Request

The Certificate Signing Request (CSR) section provides an automated way of obtaining and installing a CA signed SSL server certificate.



To perform this operation do the following:

1. Click **Create CSR**. The following dialog box appears:



2. Fill in the form – with entries that are valid for your site – according to the example information in the following table:

Information	Example
Country (2 letter code)	TW
State or Province	Taiwan
Locality	Taipei
Organization	Your Company, Ltd.
Unit	Tech Department
Common Name	mycompany.com **Note:** This must be the exact domain name of the site that you want the certificate to be valid for. If the site's domain name is *www.mycompany.com*, and you only specify *mycompany.com*, the certificate will not be valid.
Email Address	administrator@yourcompany.com

3. After filling in the form (all fields are required), click **Create**.

   A self-signed certificate based on the information you just provided is now stored on the CCVSR.

4. Click Get CSR, and save the certificate file (*csr.cer*) to a convenient location on your computer.

   This is the file that you give to the third party CA to apply for their signed SSL certificate.

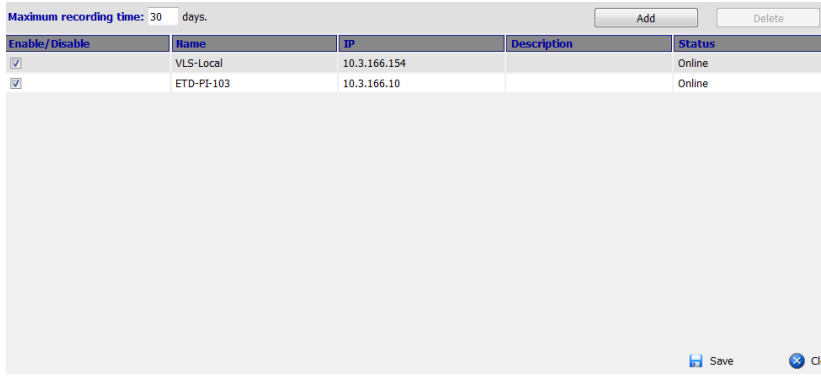
5. After the CA sends you the certificate, save it to a convenient location on your computer. Click **Browse** to locate the file; then click **Upload** to store it on the CCVSR.

Note: When you upload the file, the CCVSR checks the file to make sure the specified information still matches. If it does, the file is accepted; if not, it is rejected.

If you want to remove the certificate (to replace it with a new one because of a domain name change, for example), simply click **Remove CSR**.

Video Session Recorder

The *Video Session Recorder* page is used to add *Secondary VSR Servers* available on the network, so that you can manage them. *Secondary VSR Servers* are used to save video log files on alternative computers in order to consolidate disk space across different computers. To configure a secondary computer to work as a *Secondary VSR Server*, see *Settings*, page 15 for details. When you select *Video Session Recorder* from the *System Management* menu bar, the following screen appears:



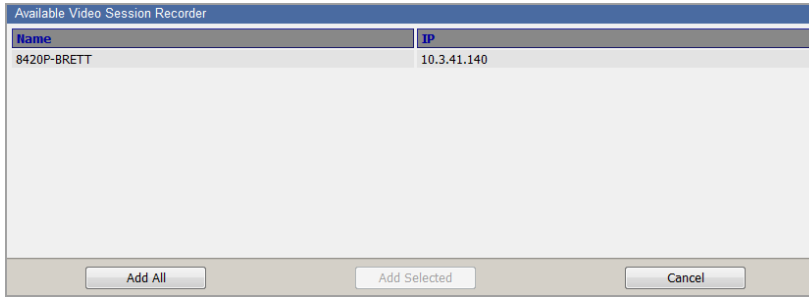
From the *Video Session Recorder* menu page you can:

- *Add* or *Delete* VSR Servers
- *Enable* or *Disable* VSR Servers
- Set the *Maximum Recording Time*

Adding Secondary VSR Servers

Adding Secondary VSR Severs allows you to configure their *Log Server Settings*. The Secondary VSR Server you are adding must be on a computer available over the network. To add a VSR Server, do the following:

1. Click **Add**. A pop-up screen appears:



2. Select a VSR Server from the list and click **Add Selected**, or click **Add All**.
3. The VSR Server will now appear on the main page and sidebar list.

Deleting Secondary VSR Servers

To delete a VSR server, do the following:

1. Select a VSR Server from the list.
2. Click **Delete**.

Enable/Disable Secondary VSR Servers

To enable/disable a VSR server, do the following:

1. Select the VSR Server from the main page, check to *Enable*, or uncheck to *Disable*, and click **Save**.

Maximum Recording Time

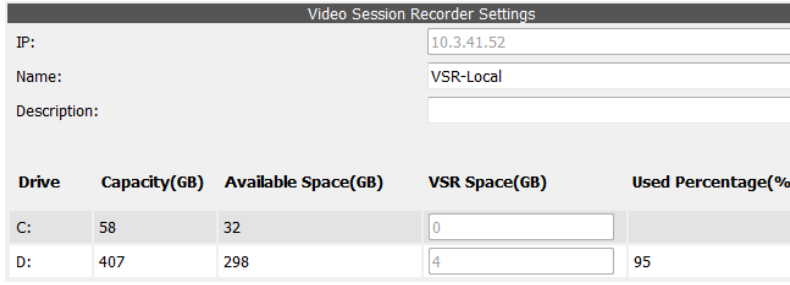
This option protects video files for the [past] number of days entered- from being overwritten. The option can be set anywhere between 3~180 days. Setting the maximum recording time tells the Video Session Recorder how many days of video files to save if the disk becomes full and the Video Session Recorder needs to overwrite old files. The default setting is 30 days.

For example, if you set the maximum recording time to 7 days, and after 14 days the disk becomes full, the Video Session Recorder will over-write *only* the oldest video files - that are older then 7 days; and leaves all video files created in the past 7 days untouched.

Log Servers

The Log Servers lists Secondary VSR Servers in the sidebar which have been added from the *Video Session Recorder* menu bar (see *Adding Secondary VSR Servers*, page 81).

Selecting a Secondary VSR Server from the sidebar list brings up the *Video Session Recorder Settings* page for that server, as shown and described below:



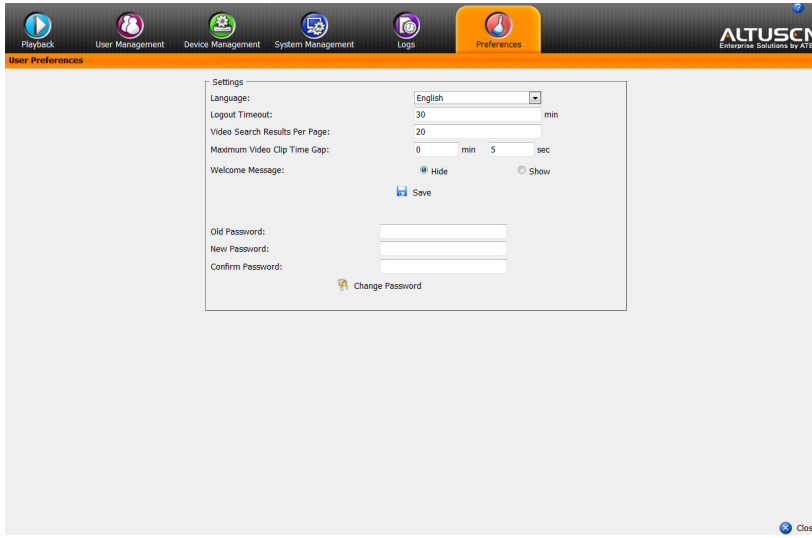
The page settings are explained in the following table:

Item	Description
IP	Displays the IP address of the Video Session Recorder.
Name	This field allows you to enter a name for the Video Session Recorder.
Description	This field allows you to enter additional information about the Video Session Recorder that you may wish to include.
Drive	The *Drive* column lists the local disks available for storing video logs.
Capacity	The *Capacity* column shows the total amount of disk space available when the drive is empty.
Available Space	The Available Space column shows the amount of disk space currently available to store data on the drive, in gigabytes.
VSR Space	In this field enter the maximum amount of space you want the Video Session Recorder to use to store recorded video logs on the drive. If the video logs exceed the VSR Space provided, the Video Session Recorder will stop recording video logs until more space is made available. If the Available Space is less then 2 GB's the VSR will create an event log notification – when the *Disk Full* event is enabled on the Logs - *Notification Settings* page (see *Notification Settings*, page 65 for details).
Used Percentage	Displays the percentage of VSR Space being used.

Chapter 11
Preferences

Overview

The *Preferences* tab allows users to set up their own individual working environments. The Video Session Recorder stores a separate configuration record for each user profile, and sets up the working configuration according to the Username that was keyed into the Login dialog box:



The page settings are explained in the following table:

Settings	Function
Language	The drop-down menu allows you to change the language of the CCVSR interface. The choices are *English*, *Chinese (Simplified)*, *Chinese (Traditional)*, *Japanese*, *Korean*.
Logout Timeout	If there is no user input for the amount of time set with this function, the user is automatically logged out. A login is necessary before the Video Session Recorder can be accessed again. The default is 30 minutes.

Settings	Function
Video Search Results Per Page	This sets the number of search results that will appear after submitting video log searches from the Playback tab. Key in a value from 20–100. The default is 20 search results.
Maximum Video Clip Time Gap	Specify the maximum amount of time in *Minutes/ Seconds* that can go by with no action on a port before the Video Session Recorder pauses recording. The moment action continues, the Video Session Recorder will resume recording, and generate a single seamless video log file. The default is 5 seconds.
Welcome Message	You can choose to *Hide* or *Show* the welcome message displayed in the submenu bar. The default is disabled.
Change Password	To change a user's password, key in the old password and new password into their input boxes; key the new password into the Confirm input box, then click *Change Password* to apply the change.

Appendix

Safety Instructions

General

- Read all of these instructions. Save them for future reference.
- Follow all warnings and instructions marked on the device.
- Do not place the device on any unstable surface (cart, stand, table, etc.). If the device falls, serious damage will result.
- Do not use the device near water.
- Do not place the device near, or over, radiators or heat registers.
- The device cabinet is provided with slots and openings to allow for adequate ventilation. To ensure reliable operation, and to protect against overheating, these openings must never be blocked or covered.
- The device should never be placed on a soft surface (bed, sofa, rug, etc.) as this will block its ventilation openings. Likewise, the device should not be placed in a built in enclosure unless adequate ventilation has been provided.
- Never spill liquid of any kind on the device.
- Unplug the device from the wall outlet before cleaning. Do not use liquid or aerosol cleaners. Use a damp cloth for cleaning.
- The device should be operated from the type of power source indicated on the marking label. If you are not sure of the type of power available, consult your dealer or local power company.
- The device is designed for IT power distribution systems with 230V phase-to-phase voltage.
- To prevent damage to your installation it is important that all devices are properly grounded.
- The device is equipped with a 3-wire grounding type plug. This is a safety feature. If you are unable to insert the plug into the outlet, contact your electrician to replace your obsolete outlet. Do not attempt to defeat the purpose of the grounding-type plug. Always follow your local/national wiring codes.
- Do not allow anything to rest on the power cord or cables. Route the power cord and cables so that they cannot be stepped on or tripped over.

- If an extension cord is used with this device make sure that the total of the ampere ratings of all products used on this cord does not exceed the extension cord ampere rating. Make sure that the total of all products plugged into the wall outlet does not exceed 15 amperes.
- To help protect your system from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply (UPS).
- Position system cables and power cables carefully; Be sure that nothing rests on any cables.
- Never push objects of any kind into or through cabinet slots. They may touch dangerous voltage points or short out parts resulting in a risk of fire or electrical shock.
- Do not attempt to service the device yourself. Refer all servicing to qualified service personnel.
- If the following conditions occur, unplug the device from the wall outlet and bring it to qualified service personnel for repair.
  - The power cord or plug has become damaged or frayed.
  - Liquid has been spilled into the device.
  - The device has been exposed to rain or water.
  - The device has been dropped, or the cabinet has been damaged.
  - The device exhibits a distinct change in performance, indicating a need for service.
  - The device does not operate normally when the operating instructions are followed.
- Only adjust those controls that are covered in the operating instructions. Improper adjustment of other controls may result in damage that will require extensive work by a qualified technician to repair.
- Do not connect the RJ-11 connector marked “UPGRADE” to a public telecommunication network.

Technical Support

International

- For online technical support – including troubleshooting, documentation, and software updates: **http://support.aten.com**
- For telephone support, see *Telephone Support*, page iii.

North America

Email Support		support@aten-usa.com
Online Technical Support	Troubleshooting Documentation Software Updates	http://www.aten-usa.com/support
Telephone Support		1-888-999-ATEN ext 4988

When you contact us, please have the following information ready beforehand:

- Product model number, serial number, and date of purchase.
- Your computer configuration, including operating system, revision level, expansion cards, and software.
- Any error messages displayed at the time the error occurred.
- The sequence of operations that led up to the error.
- Any other information you feel may be of help.

USB Authentication Key Specifications

Function		Key
Environment	Operating Temp.	0–40° C
	Storage Temp.	-20–60° C
	Humidity	0–80% RH, Non-condensing
Physical Properties	Composition	Metal and Plastic
	Weight	14 g
	Dimensions	8.36 x 2.77 x 1.37cm

Supported KVM Over the NET™ Switches

Supported KVM Switches that the Video Log Sever requires to record port access connections for the creation of video logs, include the following:

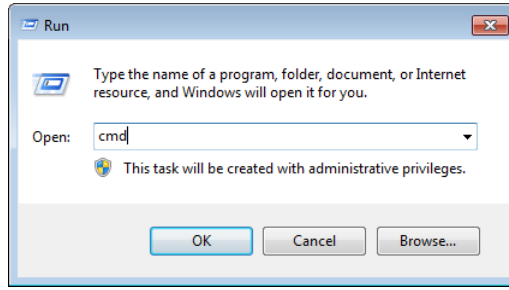
- KN2116A / KN2132 / KN4116 / KN4132
- KN2116v / KN2132v / KN4116v / KN4132v
- KN2124v / KN4124v / KN2140v / KN4140v
- KN1108v / KN1116v

Note: These are the supported devices available when the user manual was initially published. Please visit our web page to see if additional devices have been added since this manual was published**.**

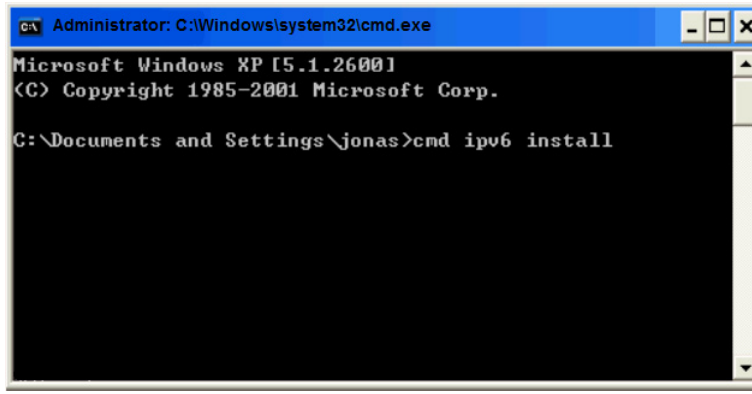
Windows XP Installation

If you are installing the CCVSR on a computer running Windows XP you need to install *IPv6* first. To install IPv6 on Windows XP, do the following;

1. Click the Start Menu - Run, and the following screen appears:


Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
cmd
This task will be created with administrative privileges.
OK
Cancel
Browse...

2. In the text box type: "*cmd*", and click **OK**. A command prompt appears:

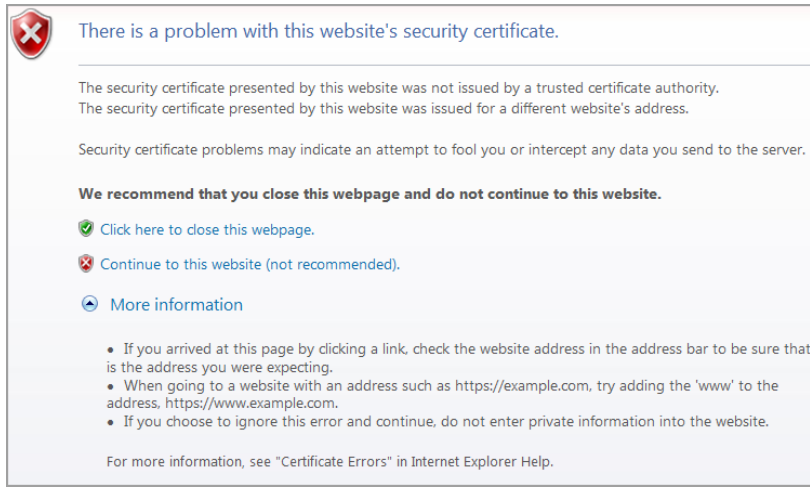

Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows XP [5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\jonas>cmd ipv6 install

3. At the command prompt type: "*cmd ipv6 install"* and press **[Enter]**.
4. IPv6 will automatically install and you can continue with the CCVSR installation on page 7.

Trusted Certificates

Overview

When you try to log in to the device from your browser, a Security Alert message appears to inform you that the device's certificate is not trusted, and asks if you want to proceed.


There is a problem with this website's security certificate.
The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.
We recommend that you close this webpage and do not continue to this website.
Click here to close this webpage.
Continue to this website (not recommended).
More information
If you arrived at this page by clicking a link, check the website address in the address bar to be sure that it is the address you were expecting.
When going to a website with an address such as https://example.com, try adding the 'www' to the address, https://www.example.com.
If you choose to ignore this error and continue, do not enter private information into the website.
For more information, see "Certificate Errors" in Internet Explorer Help.

The certificate can be trusted, but the alert is triggered because the certificate's name is not found on the Microsoft list of Trusted Authorities. You can ignore the warning and click:

Self-Signed Private Certificates

If you wish to create your own self-signed encryption key and certificate, a free utility – openssl.exe – is available for download over the web at www.openssl.org. To create your private key and certificate do the following:

1. Go to the directory where you downloaded and extracted *openssl.exe* to.
2. Run openssl.exe with the following parameters:

```
openssl req -new -newkey rsa:1024 -days 3653 -nodes -x509
-keyout CA.key -out CA.cer -config openssl.cnf.
```

Note: 1. The command should be entered all on one line (i.e., do not press [Enter] until all the parameters have been keyed in).

2. If there are spaces in the input, surround the entry in quotes (e.g. ”ATEN International”).

To avoid having to input information during key generation the following additional parameters can be used:

```
/C /ST /L /O /OU /CN /emailAddress.
```

Examples

```
openssl req -new -newkey rsa:1024 -days 3653 -nodes -x509
-keyout CA.key  -out CA.cer -config openssl.cnf -subj
/C=yourcountry/ST=yourstateorprovince/L=yourlocationor
city/O=yourorganiztion/OU=yourorganizationalunit/
CN=yourcommonname/emailAddress=name@yourcompany.com
```

```
openssl req -new -newkey rsa:1024 -days 3653 -nodes -x509
-keyout CA.key  -out CA.cer -config openssl.cnf -subj
/C=CA/ST=BC/L=Richmond/O="ATEN International"/OU=ATEN
/CN=ATEN/emailAddress=eservice@aten.com.tw
```

Importing the Files

After the openssl.exe program completes, two files – CA.key (the private key) and CA.cer (the self-signed SSL certificate) – are created in the directory that you ran the program from. These are the files that you upload in the *Private Certificate* panel of the Security page (See *Security*, page 74, and *Private Certificate*, page 78).

Limited Warranty

ALTUSEN warrants this product against defects in material or workmanship for a period of one (1) year from the date of purchase. If this product proves to be defective, contact ALTUSEN's support department for repair or replacement of your unit. ALTUSEN will not issue a refund. Return requests can not be processed without the original proof of purchase.

When returning the product, you must ship the product in its original packaging or packaging that gives an equal degree of protection. Include your proof of purchase in the packaging and the RMA number clearly marked on the outside of the package.

This warranty becomes invalid if the factory-supplied serial number has been removed or altered on the product.

This warranty does not cover cosmetic damage or damage due to acts of God, accident, misuse, abuse, negligence or modification of any part of the product. This warranty does not cover damage due to improper operation or maintenance, connection to improper equipment, or attempted repair by anyone other than ALTUSEN. This warranty does not cover products sold AS IS or WITH FAULTS.

IN NO EVENT SHALL ALTUSEN'S LIABILITY EXCEED THE PRICE PAID FOR THE PRODUCT. FURTHER, ALTUSEN SHALL NOT BE RESPONSIBLE FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE PRODUCT, ITS ACCOMPANYING SOFTWARE, OR ITS DOCUMENTATION. ALTUSEN SHALL NOT IN ANY WAY BE RESPONSIBLE FOR, WITHOUT LIMITATION, LOSS OF DATA, LOSS OF PROFITS, DOWNTIME, GOODWILL, DAMAGE OR REPLACEMENT OF EQUIPMENT OR PROPERTY, AND ANY EXPENSES FROM RECOVERY, PROGRAMMING, AND REPRODUCTION OF ANY PROGRAM OR DATA.

ALTUSEN makes no warranty or representation, expressed, implied, or statutory with respect to its products, contents or use of this documentation and all accompanying software, and specifically disclaims its quality, performance, merchantability, or fitness for any particular purpose.

ALTUSEN reserves the right to revise or update its product, software or documentation without obligation to notify any individual or entity of such revisions, or update.

For details about extended warranties, please contact one of our dedicated value added resellers.